

Name: Irfan Kamate
USN: 2GI19CS052

Assignment-1

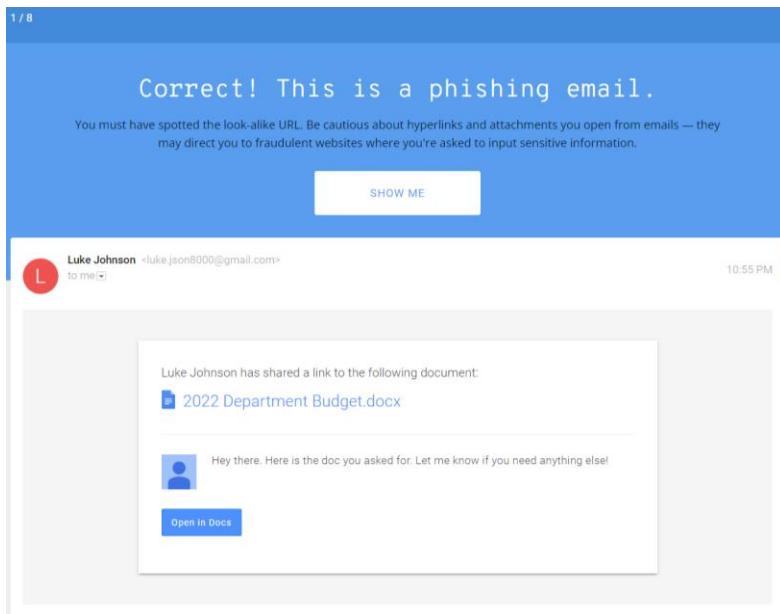
Activity - 1

Task: Identify the following mails are “Phishing” or “Legitimate”

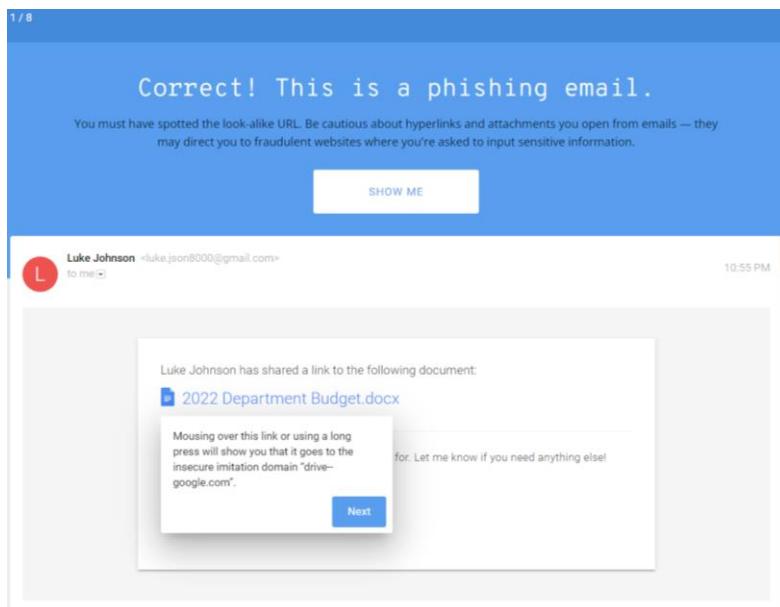
Phishing: an attack that attempts to steal your money, or your identity, by getting you to reveal personal information - such as credit card numbers, bank information, or passwords - on websites that pretend to be legitimate.

Legitimate: something legal or acceptable.

Problem 1:



Reason:



Problem 2:

2 / 8

Correct! This is a phishing email.

Well spotted! As you saw, the sender's email domain is misspelled as "efacks" and the link actually points to "mailru382.co". Phishing often tries to trick you with look-alike URLs.

[SHOW ME](#)

Fax Message NoReply [admin] <noreply@efacks.com>
to me ↗ 10:57 PM

You have received a 1 page fax at 11/23/22, 10:57 PM
[Click here to view this fax online](#)



Thank you for using the eFax Service! Please visit www.efax.com/en/efax/page/help if you have any questions, or believe you have received this fax in error.
eFax Inc (c) 2022

Reason:

2 / 8

Correct! This is a phishing email.

Well spotted! As you saw, the sender's email domain is misspelled as "efacks" and the link actually points to "mailru382.co". Phishing often tries to trick you with look-alike URLs.

[SHOW ME](#)

Fax Message NoReply [admin] <noreply@efacks.com>
to me ↗ 10:57 PM

The sender address is "efacks.com", which is misspelled. On the next question, try exploring the header for more details.

[Next](#)



Thank you for using the eFax Service! Please visit www.efax.com/en/efax/page/help if you have any questions, or believe you have received this fax in error.
eFax Inc (c) 2022

Problem 3:

3 / 8

Correct! This is a phishing email.

Looks like you spotted the look-alike URL. The real domain is "sytez.net", which is disguised to look like Google Drive.
Remember to be especially cautious if you aren't sure you know the sender.

[SHOW ME](#)



TK <tk867530@gmail.com>
to me

7:37 AM

hey, do you remember [THIS PHOTO!](#)

Reason:

3 / 8

Correct! This is a phishing email.

Looks like you spotted the look-alike URL. The real domain is "sytez.net", which is disguised to look like Google Drive.
Remember to be especially cautious if you aren't sure you know the sender.

[SHOW ME](#)



TK <tk867530@gmail.com>
to me

7:37 AM

hey, do you remember [THIS PHOTO!](#)

The link URL actually points to "sytez.net",
not Google Drive.

[Next](#)

Problem 4:

4 / 8

Correct!

This is a legitimate Dropbox communication. The sender is "dropboxmail.com", which is unusual but legitimate, and the URL is a secure link (<https://dropbox.com>).

[SHOW ME](#)

D Dropbox <no-reply@dropboxmail.com>
to me 7:38 AM

Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

[Upgrade your Dropbox](#)

For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, check out [Dropbox for Business](#).

Reason:

4 / 8

Correct!

This is a legitimate Dropbox communication. The sender is "dropboxmail.com", which is unusual but legitimate, and the URL is a secure link (<https://dropbox.com>).

[SHOW ME](#)

D Dropbox <no-reply@dropboxmail.com>
to me 7:38 AM

A quick search for "dropboxmail.com" will show that it's legitimate.

[Next](#)

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

[Upgrade your Dropbox](#)

For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, check out [Dropbox for Business](#).

4 / 8

Correct!

This is a legitimate Dropbox communication. The sender is "dropboxmail.com", which is unusual but legitimate, and the URL is a secure link (<https://dropbox.com>).

[SHOW ME](#)

D Dropbox <no-reply@dropboxmail.com>
to me 7:38 AM

Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

[Upgrade your Dropbox](#)

The URL is a legitimate, secure link to "dropbox.com".

[Next](#)

For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, check out [Dropbox for Business](#).

Problem 5:

5 / 8

Correct! This is a phishing email.

This was a complicated phish! PDFs can contain malware or viruses — always be certain you trust the sender and use your browser or an online service such as Google Drive to open them safely.

[SHOW ME](#)

Sharon Mosley <sharon.mosley@westmountdayschool.org>
to me ↗ 7:40 AM

Good day Irfan K,

Please find attached the 2022 financial activity report for your perusal.

Thanks & Regards,

Ms. Sharon Mosley
Westmount Day School

 PDF

 2022 F.A.R.pdf

Reason:

5 / 8

Correct! This is a phishing email.

This was a complicated phish! PDFs can contain malware or viruses — always be certain you trust the sender and use your browser or an online service such as Google Drive to open them safely.

[SHOW ME](#)

Sharon Mosley <sharon.mosley@westmountdayschool.org>
to me ↗ 7:40 AM

The from address is slightly different from what you'd seen in the past: "sharon.mosley@westmountschool.org".

Good day Irfan K,

Please find attached the 2022 financial activity report for your perusal.

Thanks & Regards,

Ms. Sharon Mosley
Westmount Day School

 PDF

 2022 F.A.R.pdf

Correct! This is a phishing email.

This was a complicated phish! PDFs can contain malware or viruses — always be certain you trust the sender and use your browser or an online service such as Google Drive to open them safely.

[SHOW ME](#)

Sharon Mosley <sharon.mosley@westmountdayschool.org>
to me ↗ 7:40 AM

Good day Irfan K,

Please find attached the 2022 financial activity report for your perusal.

Thanks & Regards,

Ms. Sharon Mosley
Westmount Day School

 PDF

 2022 F.A.R.pdf

Be careful when opening PDFs, especially if you don't expect them.

[Next](#)

Privacy / Terms / Feedback

Problem 6:

6 / 8

Correct. This email used a look-alike URL.

This is almost identical to an attack used to successfully hack politicians' emails. Always be sure to check URLs carefully!

[SHOW ME](#)

 Google <no-reply@google.support>
to me

10:59 PM

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Wednesday, November 23, 2022 at 10:59:09 PM GMT+05:30
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

[CHANGE PASSWORD](#)

Best,
The Mail Team

Reason:

6 / 8

Correct. This email used a look-alike URL.

This is almost identical to an attack used to successfully hack politicians' emails. Always be sure to check URLs carefully!

[SHOW ME](#)

 Google <no-reply@google.support>
to me

10:59 PM

The sender address "google.support" isn't used.

[Next](#)

So

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Wednesday, November 23, 2022 at 10:59:09 PM GMT+05:30
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

[CHANGE PASSWORD](#)

Best,
The Mail Team

6 / 8

Correct. This email used a look-alike URL.

This is almost identical to an attack used to successfully hack politicians' emails. Always be sure to check URLs carefully!

[SHOW ME](#)

 Google <no-reply@google.support>
to me

10:59 PM

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Wednesday, November 23, 2022 at 10:59:09 PM GMT+05:30
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

[CHANGE PASSWORD](#)

This link points to a subdomain of "ml-security.org", not Google.

[Next](#)

Problem 7:

7 / 8

Correct. This is based on a real warning but links to a fake login page.

The hackers tried to use Google to hide the actual link, which is from tinyurl. An email similar to this was used to target think tanks and politicians.

[SHOW ME](#)

 Google <no-reply@google.support>
to me 11:00 PM



Government-backed attackers may be trying to steal your password

There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:

[Change password](#)

Reason:

7 / 8

Correct. This is based on a real warning but links to a fake login page.

The hackers tried to use Google to hide the actual link, which is from tinyurl. An email similar to this was used to target think tanks and politicians.

[SHOW ME](#)

 Google <no-reply@google.support>
to me 11:00 PM



As in the previous question,
"google.support" is an unused address.

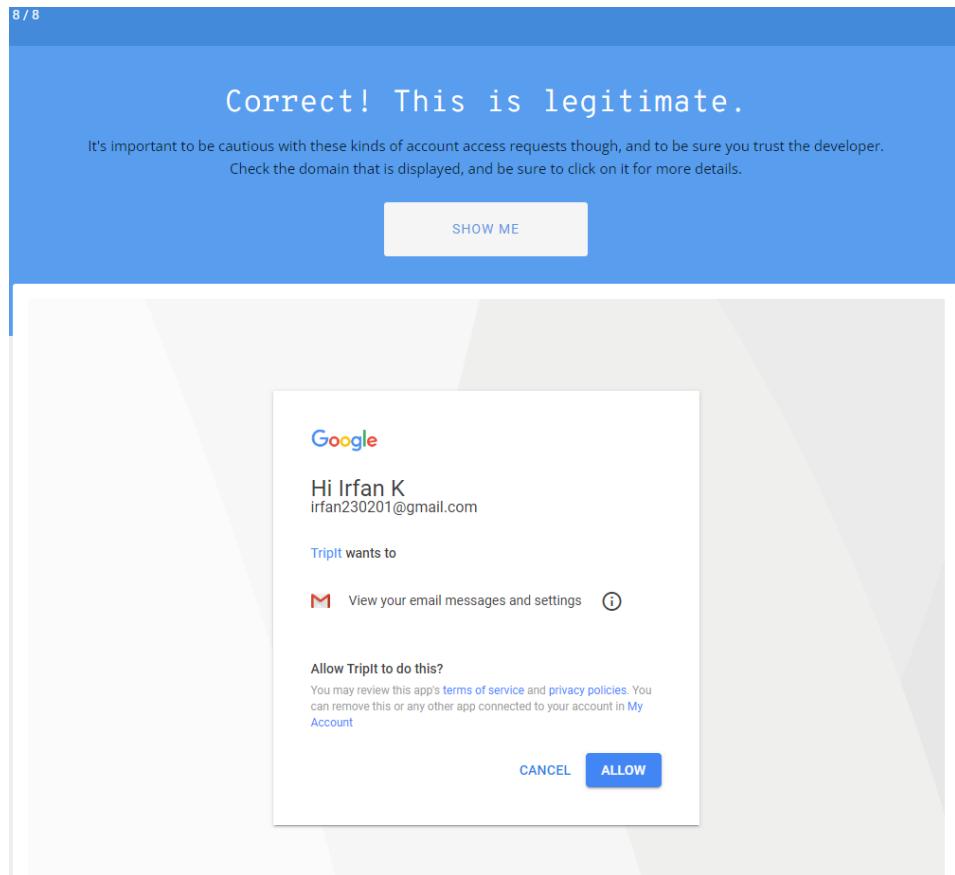
[Next](#)

Government-backed attackers may be trying to steal your password

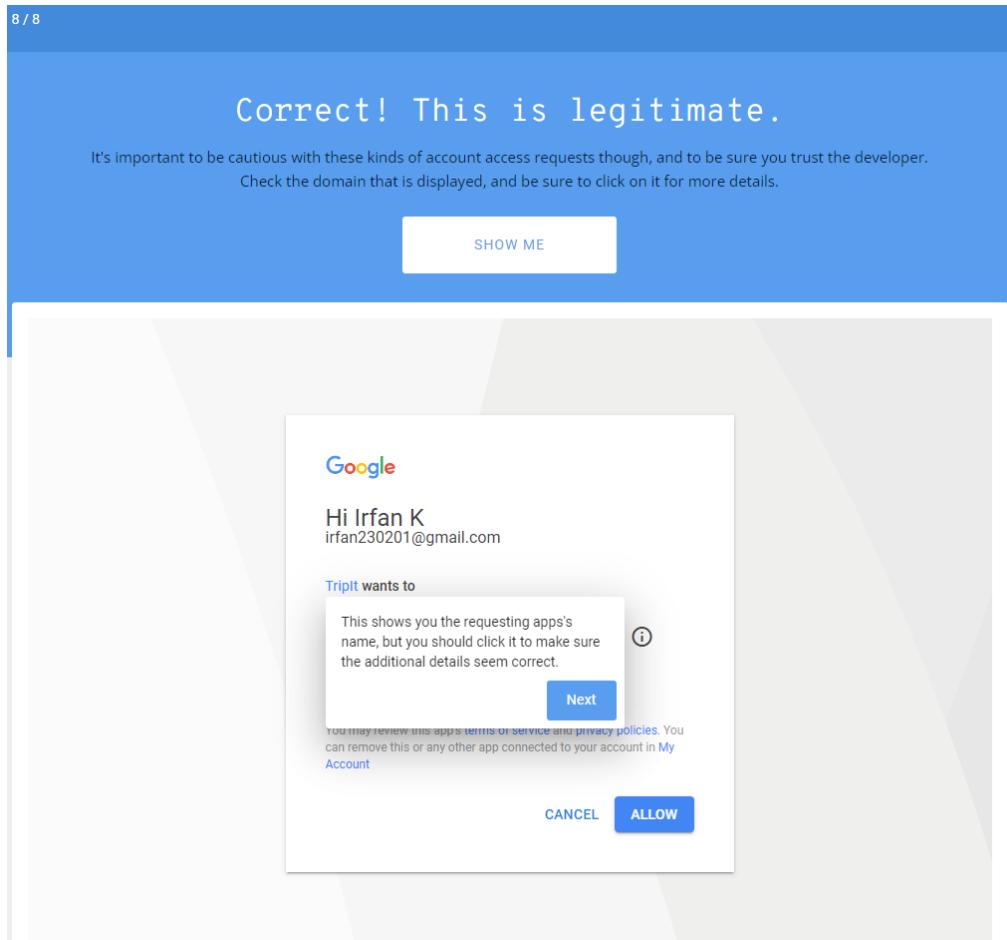
There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:

[Change password](#)

Problem 8:



Reason:



Activity – 2

Task: Compare Chrome search and Torr Browser

Chrome Browser

The screenshot shows a Google search results page for the query "ms dhoni". The top stories section features news articles from Zee News, The Indian Express, and Hindustan Times about Narendra Modi and Ravindra Jadeja. To the right, there is a table of MS Dhoni's career statistics for ODI, T20I, and IPL, followed by social media links for Instagram, Facebook, and Twitter. A "People also search for" section at the bottom right includes profiles for Dinesh Karthik, Faf du Plessis, Virat Kohli, and Sakshi Dhoni.

Format	Matches	Runs	Avg	SR
ODI	350	10773	50.6	87.6
T20I	98	1617	37.6	126.1
IPL	234	4978	39.2	135.2

Torr Browser

The screenshot shows a DuckDuckGo search results page for the query "ms dhoni". The top result is a link to Cricbuzz.com's profile of MS Dhoni, which includes his ICC Ranking, Age, Career Info & Stats. Below it is a link to ESPNcricinfo.com with information about his profile and biography. Further down is a link to Britannica.com's biography of M.S. Dhoni. The bottom result is a link to IMDb.com for Mahendra Singh Dhoni.

Activity – 3

Google Search Operators

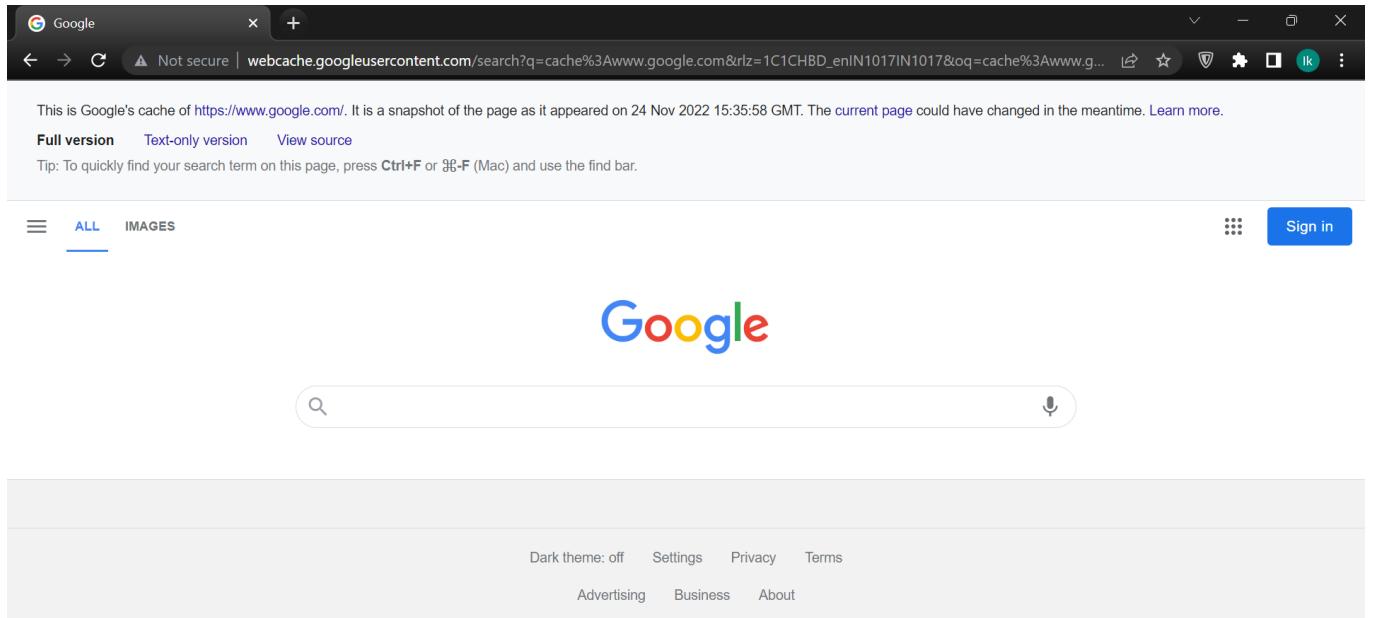
1. intitle

The screenshot shows a Google search results page with the query "intitle:password site:www.eccouncil.org". The results are filtered to show only one result, which is a link to a "Password Cracking Cyber Challenges Training Course" on the EC-Council website. Below the search bar, there are navigation links for All, Images, Videos, Books, Shopping, and More. The results section shows the URL and a snippet of the page content. At the bottom, there is a "View all" button and a feedback link.

2. filetype

The screenshot shows a Google search results page with the query "ec-council filetype:pdf". The results are filtered to show over 7,000,000 results. The top result is a PDF titled "Cyber-Handbook-Enterprise.pdf" from EC-Council. Below the search bar, there are navigation links for All, News, Images, Videos, Shopping, and More. The results section shows the URL and a snippet of the page content. A "People also ask" section is visible at the bottom, listing questions like "What is meant by EC-Council?", "Are EC-Council courses free?", "Who is owner of EC-Council?", and "How much does EC-Council certification cost?".

3. cache



4. allinurl

A screenshot of a web browser displaying search results for the query "allinurl: google career". The URL in the address bar is `google.com/search?q=allinurl%3A+google+career&rlz=1C1CHBD_enIN1017IN1017&oq=allinurl%3A+google+career&aqs=chrome..69i57...`. The results page is in dark mode and shows job listings for Google. The first three results are: 1) Capacity Planning Lead, Customer Engineering, Google Cloud, Bangalore, Karnataka via Google Careers (Full-time); 2) User Experience Engineer, Google, Bangalore, Karnataka via Glassdoor (10 days ago, Full-time); 3) Software Engineering Manager II, Payments, Google Inc, Bangalore, Karnataka via www.foundit.in (Full-time). A link to "26 more jobs" is also present.

5. inurl

The screenshot shows a Google search results page with the query "inurl: copy site:www.google.com". The results are as follows:

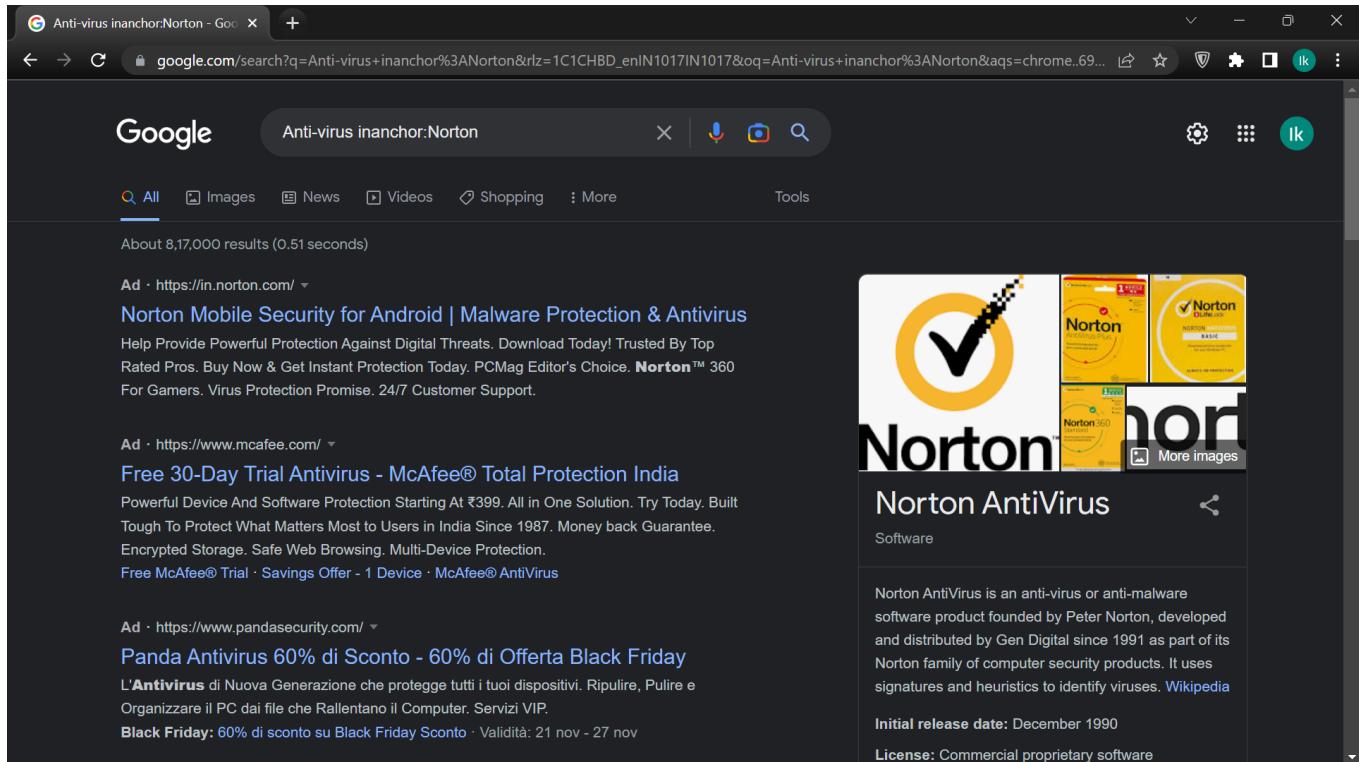
- Chrome Browser – Privacy Policy - Google**
11-Aug-2022 — If there's a match, your browser sends Google a hashed, partial **copy** of the site's **URL** so that Google can send more information to your ...
Browser modes · Managing users in Chrome · Safe Browsing practices
- Google Chrome Privacy Whitepaper**
04-Feb-2021 — The most recent **copy** of this list is stored locally on your system. Chrome checks the **URL** of each site you visit or file you download ...
Omnibox · New Tab page · Safe Browsing protection · Google update
- Google Search Appliance - Feeds Protocol Developer's Guide**
Making **copies**, adaptations, or compilation works, without prior written ... May include metadata, if the feed type is set to "metadata-and-url".
45 pages

6. allintitle

The screenshot shows a Google search results page with the query "allintitle:detect malware". The results are as follows:

- Detect Malware – Upwork Customer Service & Support**
If you suspect your computer has been infected with malware, **run a trusted antivirus program immediately**. If you don't currently have one, two options are Avast Free Antivirus or Malwarebytes.
- How to Detect Malware (with Pictures) - wikiHow**
25 steps
1. Check if your operating system is up-to-date. Updating your operating system can be annoy...
2. Check if you are getting a lot of pop-ups. If your computer has been infected by malware, y...
3. Look for new toolbar items and icons. If you see new toolbar items, browser extensions, or i...

7. inanchor



Anti-virus inanchor:Norton - Google

Anti-virus inanchor:Norton

About 8,17,000 results (0.51 seconds)

Ad · https://in.norton.com/ ▾

Norton Mobile Security for Android | Malware Protection & Antivirus

Help Provide Powerful Protection Against Digital Threats. Download Today! Trusted By Top Rated Pros. Buy Now & Get Instant Protection Today. PCMag Editor's Choice. **Norton™ 360** For Gamers. Virus Protection Promise. 24/7 Customer Support.

Ad · https://www.mcafee.com/ ▾

Free 30-Day Trial Antivirus - McAfee® Total Protection India

Powerful Device And Software Protection Starting At ₹399. All in One Solution. Try Today. Built Tough To Protect What Matters Most to Users in India Since 1987. Money back Guarantee. Encrypted Storage. Safe Web Browsing. Multi-Device Protection.

Free McAfee® Trial · Savings Offer - 1 Device · McAfee® AntiVirus

Ad · https://www.pandasecurity.com/ ▾

Panda Antivirus 60% di Sconto - 60% di Offerta Black Friday

L'Antivirus di Nuova Generazione che protegge tutti i tuoi dispositivi. Ripulire, Pulire e Organizzare il PC dai file che Rallentano il Computer. Servizi VIP.

Black Friday: 60% di sconto su Black Friday Sconto · Validità: 21 nov - 27 nov

Norton AntiVirus

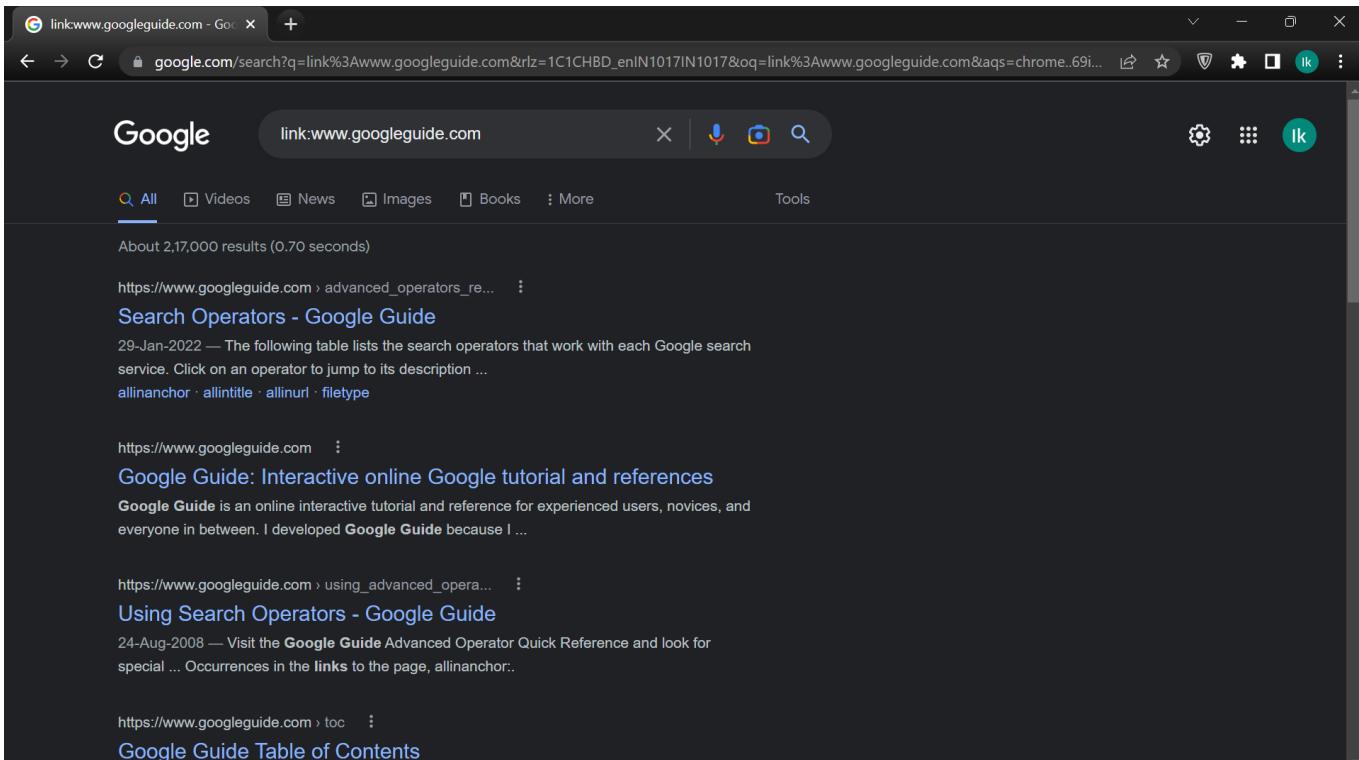
Software

Norton AntiVirus is an anti-virus or anti-malware software product founded by Peter Norton, developed and distributed by Gen Digital since 1991 as part of its Norton family of computer security products. It uses signatures and heuristics to identify viruses. [Wikipedia](#)

Initial release date: December 1990

License: Commercial proprietary software

8. link



link:www.googleguide.com - Google

link:www.googleguide.com

About 2,17,000 results (0.70 seconds)

https://www.googleguide.com/advanced_operators_re... ::

Search Operators - Google Guide

29-Jan-2022 — The following table lists the search operators that work with each Google search service. Click on an operator to jump to its description ...

[allinanchor](#) · [allintitle](#) · [allinurl](#) · [filetype](#)

<https://www.googleguide.com/> ::

Google Guide: Interactive online Google tutorial and references

Google Guide is an online interactive tutorial and reference for experienced users, novices, and everyone in between. I developed Google Guide because I ...

https://www.googleguide.com/using_advanced_opera... ::

Using Search Operators - Google Guide

24-Aug-2008 — Visit the Google Guide Advanced Operator Quick Reference and look for special ... Occurrences in the links to the page, allinanchor::

<https://www.googleguide.com/toc> ::

Google Guide Table of Contents

9. related

A screenshot of a Google search results page. The search query is "related:www.geeksforgeeks.org". The results are as follows:

- Ideone.com**
Compile various programming languages online. Add input stream, save output, add notes and tags.
- CareerCup: Programming Interview Questions**
CareerCup's interview videos give you a real-life look at technical interviews. In these unscripted videos, watch how other candidates handle tough questions ...
- LeetCode - The World's Leading Online Programming ...**
Level up your coding skills and quickly land a job. This is the best place to expand your knowledge and get prepared for your next interview.
- HackerEarth | Online coding platform and developer ...**
Helping 3M+ developers be better through coding contests, data science competitions, and

10. Thumbnail Extraction

A screenshot of a browser window titled "Extract Meta Data" showing the YouTube DataViewer extension. The URL is <https://citizenevidence.amnestyusa.org>. The page displays the following information:

AMNESTY INTERNATIONAL

Youtube DataViewer

https://www.youtube.com/watch?v=oSF8MOz_I Go Clear

Avatar: The Way of Water | New Trailer

Set more than a decade after the events of the first film, "Avatar: The Way of Water" begins to tell the story of the Sully family (Jake, Neytiri, and their kids), the trouble that follows them, the lengths they go to keep each other safe, the battles they fight to stay alive, and the tragedies they endure. Directed by James Cameron and produced by Cameron and Jon Landau, the Lightstorm Entertainment Production stars Sam Worthington, Zoe Saldana, Sigourney Weaver, Stephen Lang and Kate Winslet. Screenplay by James Cameron & Rick Jaffa & Amanda Silver. Story: James Cameron & Rick Jaffa & Amanda Silver & Josh Friedman & Shane Salerno. David Valdes and Richard Edensham serve as the film's executive producers. Get tickets now: www.fandango.com/avatarthewayofwater Twitter: @OfficialAvatar @20thCentury FBMG: @avatar @20thCenturyStudios

Video ID: oSF8MOz_I
Upload Date (YYYY/MM/DD): 2022-11-22
Upload Time (UTC): 02:53:38 (convert to local time)

Thumbnails:

Two thumbnail images are shown, both labeled "reverse image search":

- The top thumbnail shows a scene from the movie Avatar: The Way of Water.
- The bottom thumbnail shows another scene from the movie.

Assignment – 2

Activity - 1

Netcraft: Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web.

The screenshot shows a Firefox browser with a dark theme. A search for "amazon" is performed on Google. On the right, the Netcraft extension sidebar is active, showing a detailed Site Report for www.google.com. The report includes the following information:

- Risk Rating: 2
- Country: US
- Site rank: 1
- First seen: May 2002
- Host: Google LLC
- PFS: ✓
- SSLv3: Not supported

Below the report, there are buttons to "Disable protection for this site" and "Report malicious URL". A form is provided for reporting malicious URLs, with the URL <https://www.google.com/search?client=firefox-b-d&q=amazon> entered. The "Submit Report" button is visible at the bottom right of the sidebar.

The screenshot shows the Netcraft submission interface. The left sidebar displays "Submission Details" with the following information:

- SOURCE: Netcraft Extension
- SUBMITTER: irfan230201@gmail.com
- SUBMISSION DATE: 24-11-2022 21:43:00

Below this, a link "More details >" is visible. The main content area is titled "URLs" and contains the following data:

URL	Classification
https://www.google.com/search?client=firefox-b-d&q=amazon (copy to clipboard)	processing

Details for the submitted URL include:

- URL: <https://www.google.com/search?client=firefox-b-d&q=amazon>
- HOSTNAME: www.google.com
- Site Report: [Site Report](#)
- URL CLASSIFICATION LOG: URL has not yet changed state.

At the bottom, a link <https://sitereport.netcraft.com/?url=www.google.com> is shown, along with a "Privacy - Terms" link in the bottom right corner.

Activity - 2

Wappalyzer

The screenshot shows a web browser window with two tabs open. The active tab is for Amazon India, displaying a Prime membership sign-up page. A purple sidebar on the right is the Wappalyzer extension, which provides a detailed breakdown of the website's technological stack. The sidebar includes sections for Security (HSTS), Advertising (Google Ads), Miscellaneous (Open Graph), CDN (Amazon Cloudfront), and PaaS (Amazon Web Services). It also features a link for "Something wrong or missing?" and a section titled "Automate technology lookups" with sub-sections for Clothing and Footwear.

Wappalyzer analysis of the Amazon page:

- TECHNOLOGIES**
- Security**: HSTS
- Advertising**: Google Ads
- Miscellaneous**: Open Graph
- JavaScript libraries**: core-js 3.17.3, jQuery
- CDN**: Amazon Cloudfront
- PaaS**: Amazon Web Services

https://www.amazon.in/?&ext_vrn=hi&tag=googhydrabk1-21&ref=pd_sl_4d1ohbptwj_e&adgrpid=58490306106&hvpone=&hvptwo=&hvadid=486457318205&hvpos=&hvnetw=g&hvrand=14645580503197044199&hvqmt=e&hv...

Activity – 3

Kali-Linux commands

1. ifconfig

```
File Edit View Search Terminal Help
root@kali:~# ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.255.255.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 16 bytes 876 (876.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 16 bytes 876 (876.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.29.33 netmask 255.255.255.0 broadcast 192.168.29.255
                inet6 fe80::fe09:31d2%wlan0 prefixlen 64 scopeid 0x20<link>
                    inet6 2405:201:0:012:f095:31d2%wlan0 prefixlen 64 scopeid 0x0<global>
                        ether b4:69:21:d3:07:a7 txqueuelen 1000 (Ethernet)
                        RX packets 254002 bytes 363768665 (346.9 MiB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 52222 bytes 5451814 (5.1 MiB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

2. ip

```
File Edit View Search Terminal Help
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b4:69:21:d3:07:a7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.29.33/24 brd 192.168.29.255 scope global dynamic noprefixroute wlan0
            valid_lft 26138sec preferred_lft 26138sec
        inet6 2405:201:0:012:f095:31d2%wlan0 prefixlen 64 scope global dynamic noprefixroute
            valid_lft 3599sec preferred_lft 3599sec
        inet6 fe80::dec0:60b:9566:10/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@kali:~#
```

3. traceroute

```
File Edit View Search Terminal Help
root@kali:~# traceroute www.google.com
traceroute to www.google.com [142.250.182.68], 30 hops max, 60 byte packets
  1  reliance.reliance (192.168.29.1)  1.530 ms  1.590 ms  1.683 ms
  2  10.48.192.1 (10.48.192.1)  6.701 ms  6.691 ms  6.678 ms
  3  172.31.2.14 (172.31.2.14)  17.517 ms  15.721 ms  20.243 ms
  4  192.168.65.152 (192.168.65.152)  18.607 ms  192.168.65.150 (192.168.65.150)  20.706 ms  192.168.65.152 (192.168.65.152)  20.699 ms
  5  172.26.74.4 (172.26.74.4)  15.638 ms  15.635 ms  20.153 ms
  6  172.26.77.227 (172.26.77.227)  21.203 ms  172.26.77.226 (172.26.77.226)  16.241 ms  12.806 ms
  7  192.168.65.140 (192.168.65.140)  13.748 ms  192.168.65.138 (192.168.65.138)  13.714 ms  192.168.65.142 (192.168.65.142)  15.757 ms
  8  * * *
  9  * * *
10  74.125.51.4 (74.125.51.4)  26.259 ms  72.14.196.126 (72.14.196.126)  20.798 ms  26.139 ms
11  74.125.242.145 (74.125.242.145)  26.100 ms  * *
12  108.178.253.97 (108.178.253.97)  20.118 ms  142.251.55.218 (142.251.55.218)  24.988 ms  142.251.55.245 (142.251.55.245)  22.341 ms
13  108.178.253.122 (108.178.253.122)  20.454 ms  142.251.55.245 (142.251.55.245)  21.025 ms  142.251.55.247 (142.251.55.247)  22.905 ms
14  74.125.242.145 (74.125.242.145)  19.614 ms  21.998 ms  74.125.242.129 (74.125.242.129)  40.267 ms
15  maa05s20-in-f4.le100.net (142.250.182.68)  21.552 ms  39.762 ms  39.054 ms
root@kali:~# traceroute www.amazon.in
traceroute to www.amazon.in [13.249.216.298], 30 hops max, 60 byte packets
  1  reliance.reliance (192.168.29.1)  1.971 ms  1.891 ms  1.846 ms
  2  10.48.192.1 (10.48.192.1)  7.035 ms  7.001 ms  6.962 ms
  3  172.31.2.14 (172.31.2.14)  15.514 ms  19.050 ms  18.999 ms
  4  192.168.65.148 (192.168.65.148)  17.154 ms  192.168.65.150 (192.168.65.150)  18.878 ms  18.876 ms
  5  172.26.74.4 (172.26.74.4)  15.205 ms  15.191 ms  19.427 ms
  6  172.26.77.227 (172.26.77.227)  21.296 ms  172.26.77.226 (172.26.77.226)  12.026 ms  172.26.77.227 (172.26.77.227)  16.317 ms
  7  192.168.65.140 (192.168.65.140)  10.859 ms  192.168.65.144 (192.168.65.144)  13.033 ms  192.168.65.138 (192.168.65.138)  10.428 ms
  8  * * *
  9  * * *
10  99.83.67.66 (99.83.67.66)  17.693 ms  14.942 ms  14.875 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  server-13-249-216-208.blr50.r.cloudfront.net (13.249.216.208)  16.848 ms  16.810 ms  16.726 ms
root@kali:~#
```

4. netstat

```
File Edit View Search Terminal Help
root@kali:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
Active UNIX domain sockets (w/o servers)
Proto Refcnt Flags      Type      State      I-Node  Path
unix  2      [ ]      DGRAM    34828  /run/user/0/systemd/notify
unix  3      [ ]      DGRAM    14121  /run/systemd/notify
unix  2      [ ]      DGRAM    29509  /run/wpa_supplicant/wlan0
unix  6      [ ]      DGRAM    14160  /run/systemd/journal/socket
unix 12      [ ]      DGRAM    14170  /run/systemd/journal/dev-log
unix  2      [ ]      DGRAM    14213  /run/systemd/journal/syslog
unix  2      [ ]      DGRAM    33943  /run/wpa_supplicant/p2p-dev-wlan0
unix  2      [ ]      DGRAM    43590
unix  3      [ ]      STREAM   CONNECTED  35634  /run/user/0/bus
unix  3      [ ]      STREAM   CONNECTED  28350
unix  3      [ ]      STREAM   CONNECTED  38306
unix  3      [ ]      STREAM   CONNECTED  28625  @/tmp/.ICE-unix/1149
unix  3      [ ]      STREAM   CONNECTED  38275  /run/systemd/journal/stdout
unix  3      [ ]      STREAM   CONNECTED  34049  /run/user/0/bus
unix  3      [ ]      STREAM   CONNECTED  27384
unix  3      [ ]      STREAM   CONNECTED  37626
unix  3      [ ]      STREAM   CONNECTED  40100  /run/systemd/journal/stdout
unix  3      [ ]      STREAM   CONNECTED  36183  /var/run/dbus/system_bus_socket
unix  3      [ ]      STREAM   CONNECTED  38235  /run/systemd/journal/stdout
unix  3      [ ]      STREAM   CONNECTED  28505
unix  3      [ ]      STREAM   CONNECTED  36393  /var/run/dbus/system_bus_socket
unix  3      [ ]      STREAM   CONNECTED  37474  /run/systemd/journal/stdout
unix  3      [ ]      STREAM   CONNECTED  32504  /run/user/0/bus
unix  3      [ ]      STREAM   CONNECTED  43344  /run/user/0/bus
unix  3      [ ]      STREAM   CONNECTED  43022
unix  3      [ ]      STREAM   CONNECTED  30340
unix  3      [ ]      STREAM   CONNECTED  43299
```

5. dig

```
File Edit View Search Terminal Help
root@kali:~# dig google.com

; <>> DiG 9.11.5-P4-5.1+b1-Debian <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 8786
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        252     IN      A      142.250.195.46

;; Query time: 16 msec
;; SERVER: 192.168.29.1#53(192.168.29.1)
;; WHEN: Wed Nov 23 23:16:35 UTC 2022
;; MSG SIZE  rcvd: 55

root@kali:~#
```

6. nslookup

```
File Edit View Search Terminal Help
root@kali:~# nslookup amazon.com
Server:      192.168.29.1
Address:     192.168.29.1#53

Non-authoritative answer:
Name:  amazon.com
Address: 205.251.242.103
Name:  amazon.com
Address: 54.239.28.85
Name:  amazon.com
Address: 52.94.236.248

root@kali:~# nslookup google.com
Server:      192.168.29.1
Address:     192.168.29.1#53

Non-authoritative answer:
Name:  google.com
Address: 142.250.195.46
Name:  google.com
Address: 2404:6800:4007:822::200e

root@kali:~#
```

7. route

```
File Edit View Search Terminal Help
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         reliance.relian 0.0.0.0      UG    600    0      0 wlan0
192.168.29.0   0.0.0.0        255.255.255.0 U     600    0      0 wlan0
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.29.1   0.0.0.0       UG    600    0      0 wlan0
192.168.29.0   0.0.0.0        255.255.255.0 U     600    0      0 wlan0
root@kali:~# route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref  Use Iface
root@kali:~# 
```

8. arp

```
File Edit View Search Terminal Help
root@kali:~# arp
Address          Hwtype  HWaddress           Flags Mask          Iface
reliance.relian  ether    a8:da:0c:d6:48:bc C             wlan0
root@kali:~# 
```

9. whois

```
File Edit View Search Terminal Help
root@kali:~# whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2022-01-26T16:45:06Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2031-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarSAFE.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-11-23T18:01:57Z <<<
```

10. ping

```
File Edit View Search Terminal Help
root@kali:~# ping www.google.com
PING www.google.com(maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004)) 56 data bytes
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=1 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=2 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=3 ttl=59 time=18.2 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=4 ttl=59 time=18.6 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=5 ttl=59 time=18.4 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=6 ttl=59 time=18.8 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=7 ttl=59 time=18.7 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=8 ttl=59 time=26.6 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=9 ttl=59 time=19.6 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=10 ttl=59 time=19.7 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=11 ttl=59 time=19.3 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=12 ttl=59 time=25.2 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=13 ttl=59 time=23.7 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=14 ttl=59 time=29.8 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=15 ttl=59 time=34.8 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=16 ttl=59 time=27.7 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=17 ttl=59 time=27.5 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=18 ttl=59 time=21.9 ms
64 bytes from maa05s20-in-x04.le100.net (2404:6800:4007:81b::2004): icmp seq=19 ttl=59 time=31.9 ms
^C
--- www.google.com ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18038ms
rtt min/avg/max/mdev = 18.239/23.055/34.818/5.117 ms
root@kali:~# 
```

11. curl wget

```
root@kali:~# curl -O www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf
root@kali:~# wget www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf
--2022-11-23 23:29:33-- http://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf
Resolving www.ftc.gov (www.ftc.gov) ... 2405:200:1630:4ad::2031, 2405:200:1630:480::2031, 23.214.240.64
Connecting to www.ftc.gov (www.ftc.gov)[2405:200:1630:4ad::2031]:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf [following]
--2022-11-23 23:29:33-- https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf
Connecting to www.ftc.gov (www.ftc.gov)[2405:200:1630:4ad::2031]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3101899 (3.0M) [application/pdf]
Saving to: 'cybersecurity_sb_factsheets_all.pdf'

cybersecurity_sb_factsheets_all.pdf          100%[=====] 2.96M  --.KB/s   in 0.1s

2022-11-23 23:29:33 (23.0 MB/s) - 'cybersecuirty_sb_factsheets_all.pdf' saved [3101899/3101899]

root@kali:~#
```

12. host

```
File Edit View Search Terminal Help
root@kali:~# host google.com
google.com has address 142.250.195.46
google.com has IPv6 address 2404:6800:4007:822::200e
google.com mail is handled by 10 smtp.google.com.
root@kali:~# host amazon.com
amazon.com has address 52.94.236.248
amazon.com has address 54.239.28.85
amazon.com has address 205.251.242.103
amazon.com mail is handled by 5 amazon-smtp.amazon.com
root@kali:~#
```

13. hostname

```
File Edit View Search Terminal Help
root@kali:~# hostname
kali
root@kali:~# sudo hostname Cypher
root@kali:~# hostname
Cypher
root@kali:~#
```

14. iwconfig

```
File Edit View Search Terminal Help
root@kali:~# iwconfig
wlan0    IEEE 802.11  ESSID:"Shetty_5G"
          Mode:Managed Frequency:5.18 GHz  Access Point: A8:D4:0C:D6:48:BE
          Bit Rate=866.7 Mb/s  Tx-Power=22 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=70/70  Signal level=-27 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:7  Missed beacon:0

lo      no wireless extensions.

root@kali:~#
```

15. tcpdump

16. ss

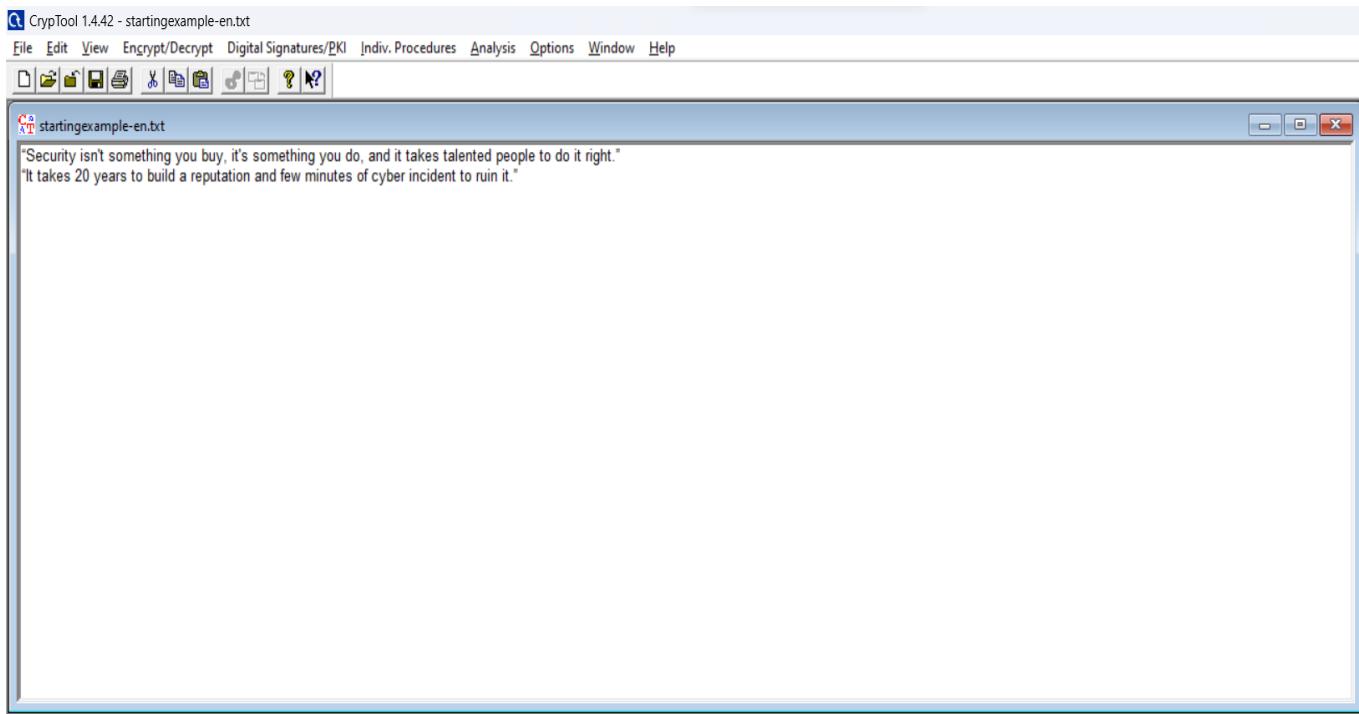
```
root@kali:~# ss
File Edit View Search Terminal Help
root@kali:~# ss
Netid      State     Recv-Q     Send-Q          Local Address:Port          Peer Address:Port
u_str      ESTAB      0          0          /run/user/0/bus 35634
u_str      ESTAB      0          0          * 28350
u_str      ESTAB      0          0          * 38306
u_str      ESTAB      0          0          @/tmp/.ICE-unix/1149 28625
u_str      ESTAB      0          0          /run/systemd/journal/stdout 38275
u_str      ESTAB      0          0          /run/user/0/bus 34049
u_str      ESTAB      0          0          * 27384
u_str      ESTAB      0          0          * 37626
u_str      ESTAB      0          0          /run/systemd/journal/stdout 40100
u_str      ESTAB      0          0          /var/run/dbus/system_bus_socket 36183
u_str      ESTAB      0          0          /run/systemd/journal/stdout 38235
u_str      ESTAB      0          0          * 28505
u_str      ESTAB      0          0          /var/run/dbus/system_bus_socket 36393
u_str      ESTAB      0          0          /run/systemd/journal/stdout 37474
u_str      ESTAB      0          0          /run/user/0/bus 32504
u_str      ESTAB      0          0          /run/user/0/bus 43344
u_str      ESTAB      0          0          * 43022
u_str      ESTAB      0          0          * 30340
u_str      ESTAB      0          0          * 43299
u_str      ESTAB      0          0          * 37650
u_str      ESTAB      0          0          /run/systemd/journal/stdout 34949
u_str      ESTAB      0          0          /run/systemd/journal/stdout 35000
u_str      ESTAB      0          0          /var/run/dbus/system_bus_socket 33308
u_str      ESTAB      0          0          /var/run/dbus/system_bus_socket 28417
u_str      ESTAB      0          0          /run/systemd/journal/stdout 36356
u_str      ESTAB      0          0          @/tmp/.X11-unix/X0 40214
u_str      ESTAB      0          0          * 27532
u_str      ESTAB      0          0          /run/user/0/bus 37427
u_str      ESTAB      0          0          /run/systemd/journal/stdout 43079
u_str      ESTAB      0          0          * 34256
u_str      ESTAB      0          0          * 27385
u_str      ESTAB      0          0          /run/systemd/journal/stdout 35068
u_str      ESTAB      0          0          /run/user/0/bus 44217
u_str      ESTAB      0          0          /var/run/dbus/system_bus_socket 35610
u_str      ESTAB      0          0          @/tmp/.X11-unix/X0 40195
u_str      ESTAB      0          0          * 45503
u_str      ESTAB      0          0          * 43353
u_str      ESTAB      0          0          * 28346
u_str      ESTAB      0          0          * 43021
u_str      ESTAB      0          0          * 36160
u_str      ESTAB      0          0          * 27389
u_str      ESTAB      0          0          * 38475
u_str      ESTAB      0          0          /run/systemd/journal/stdout 40172
u_str      ESTAB      0          0          * 36190
u_str      ESTAB      0          0          /run/user/0/pulse/native 37426
u_str      ESTAB      0          0          /run/systemd/journal/stdout 23386
u_str      ESTAB      0          0          * 43074
u_str      ESTAB      0          0          * 31382
u_str      ESTAB      0          0          /run/user/0/bus 43015
u_str      ESTAB      0          0          * 40082
u_str      ESTAB      0          0          * 32951
u_str      ESTAB      0          0          * 34193
u_str      ESTAB      0          0          * 27993

```

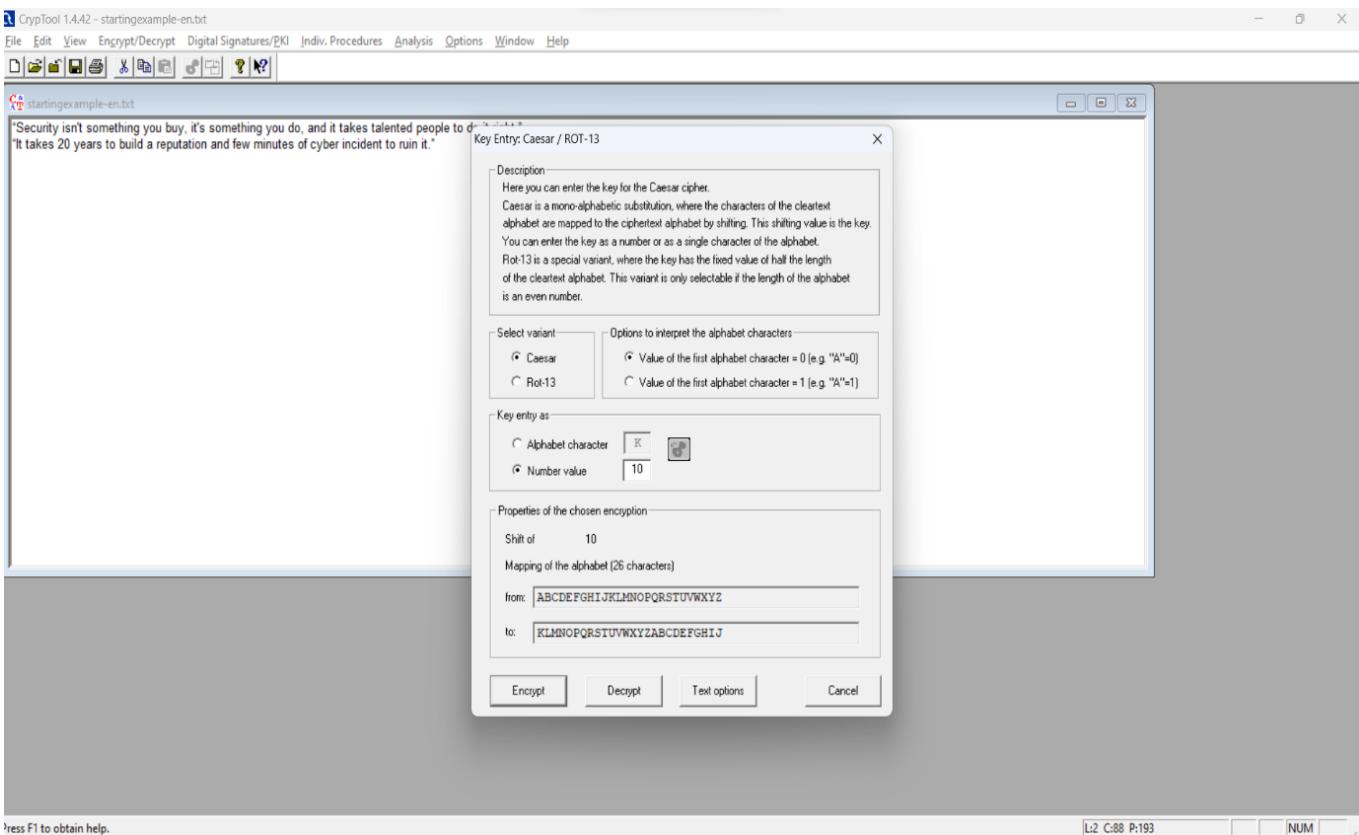
Assignment – 3

Activity – 1

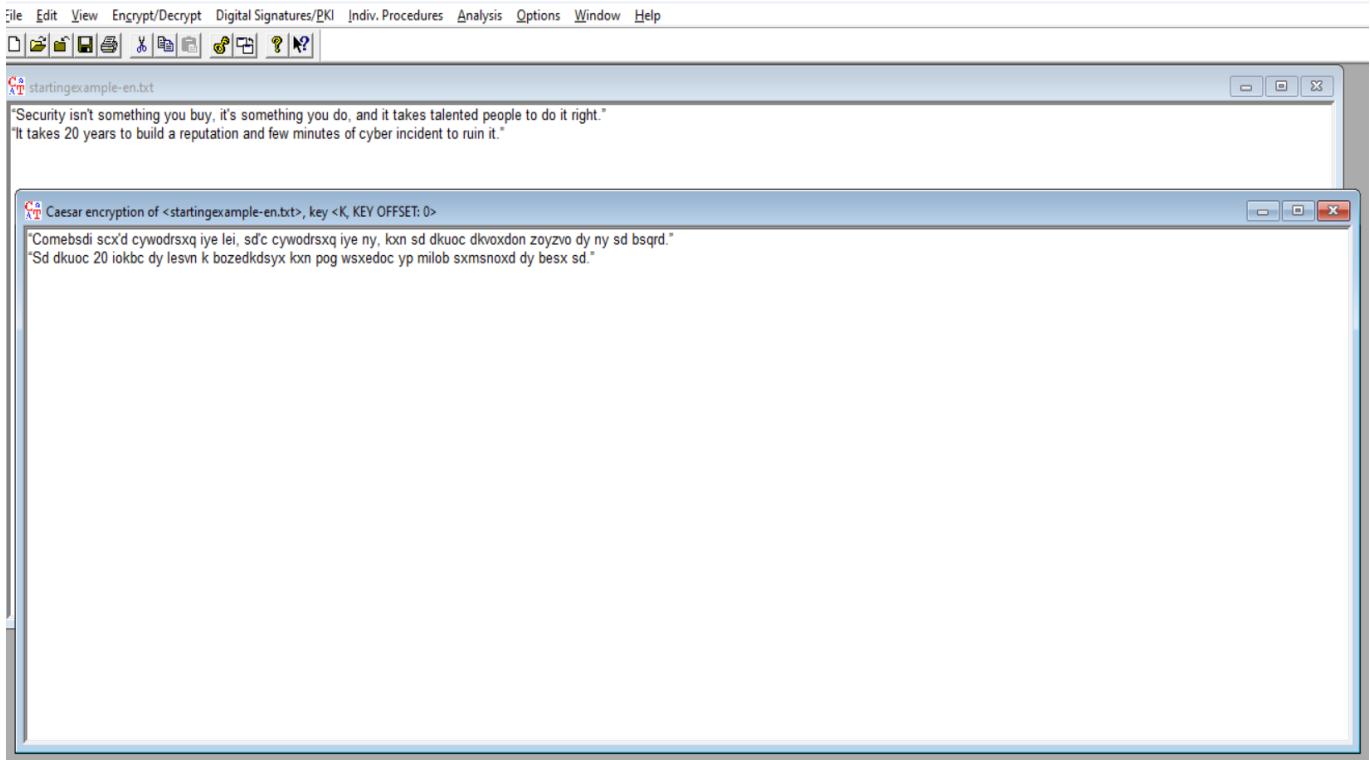
Text Message



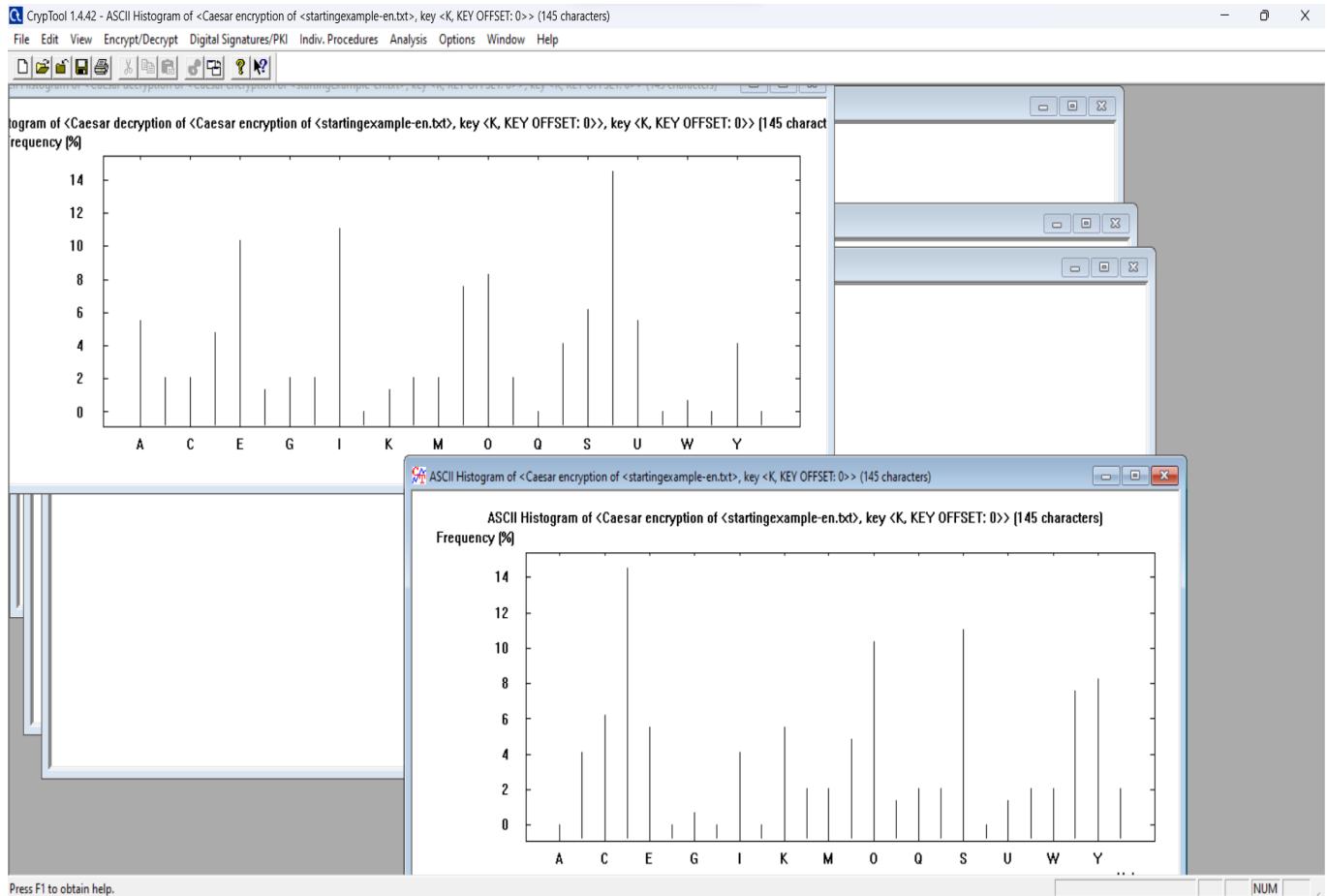
Encryption Number Value



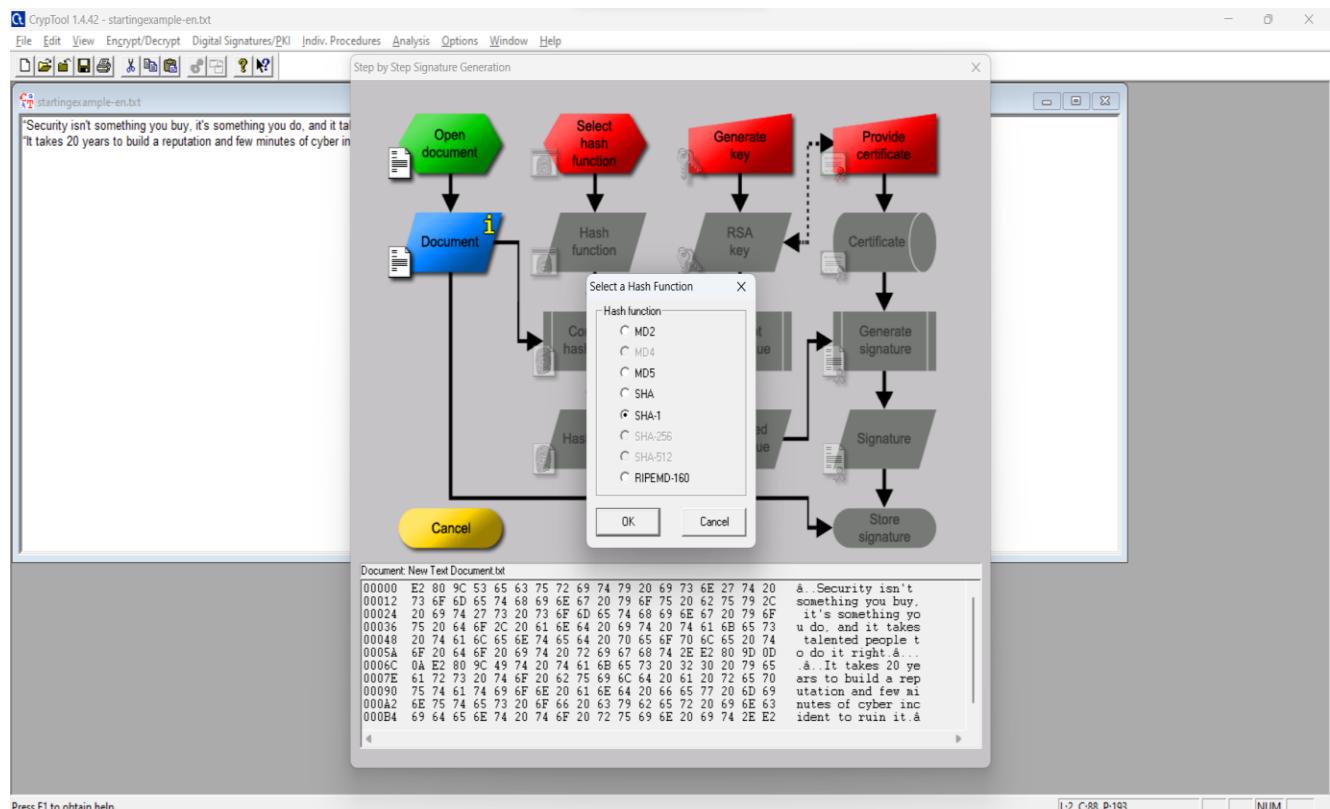
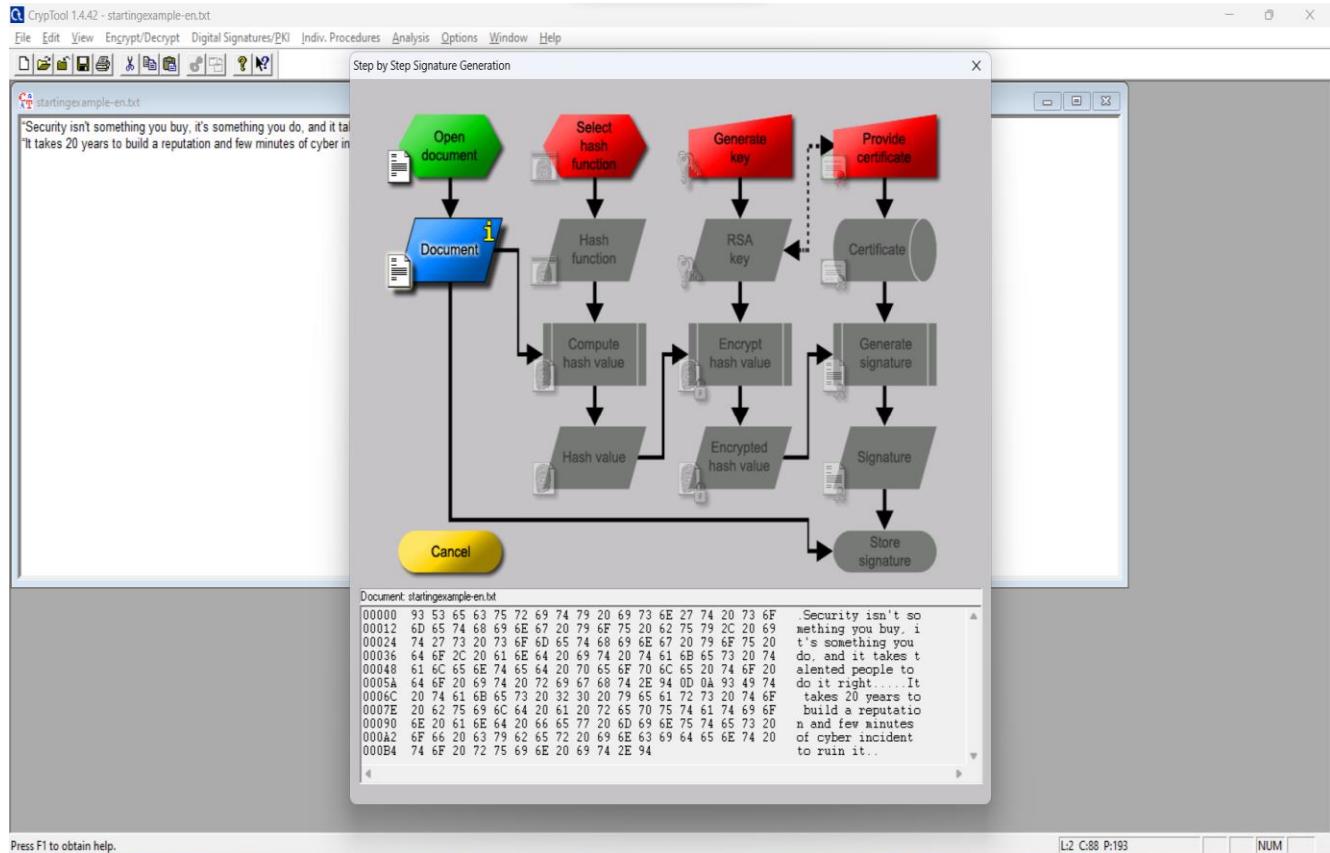
Encrypted Form of Message

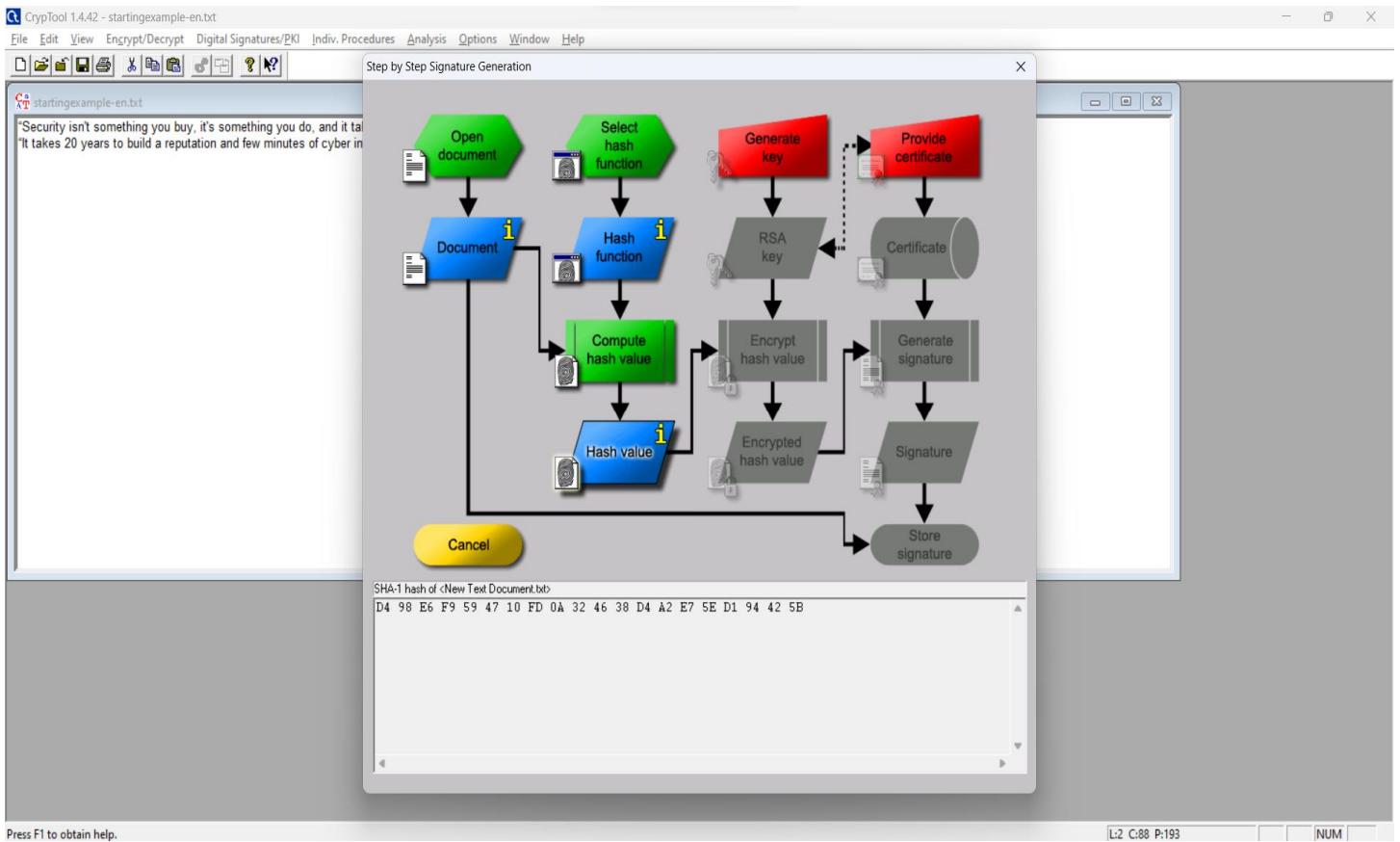
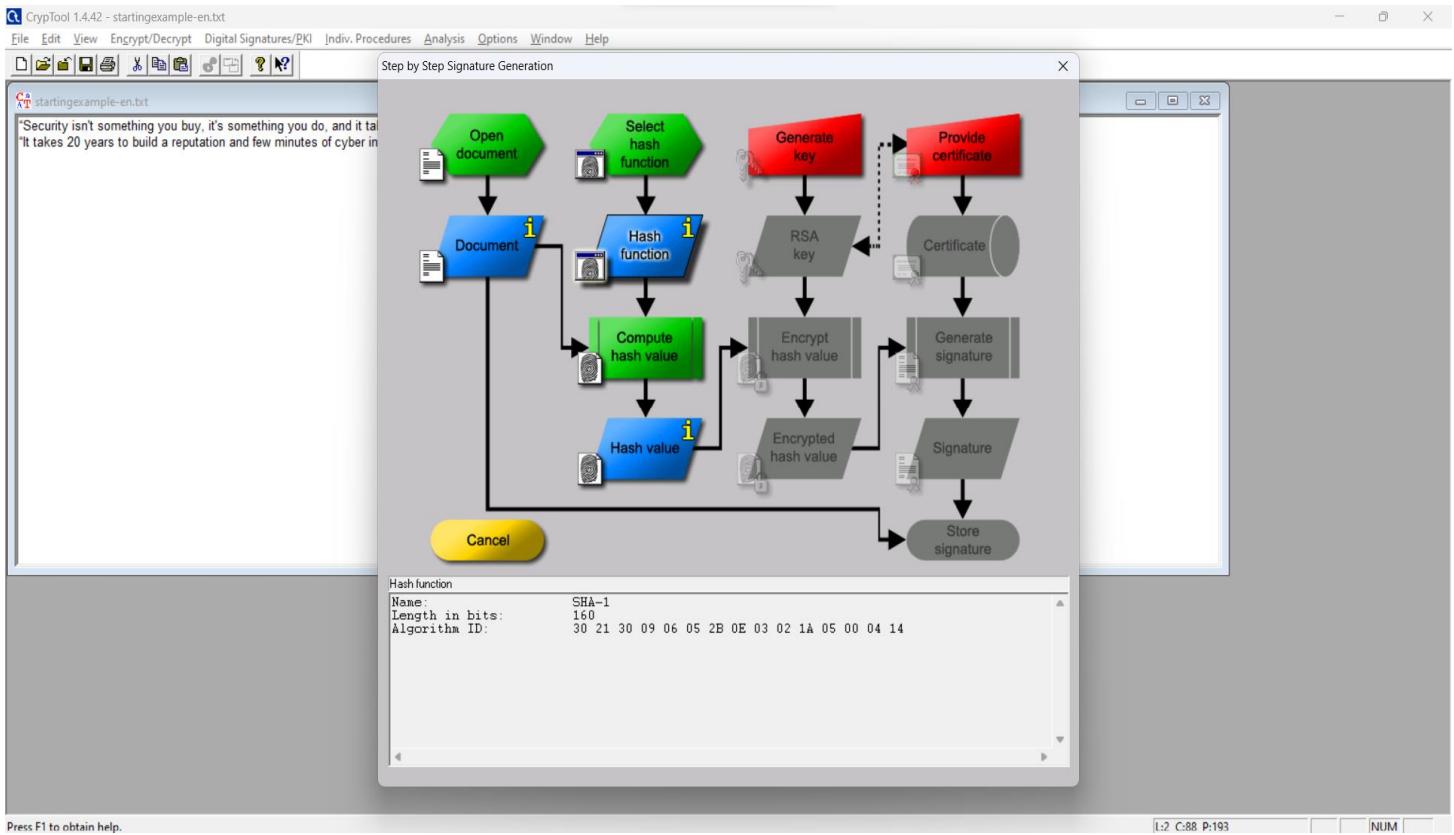


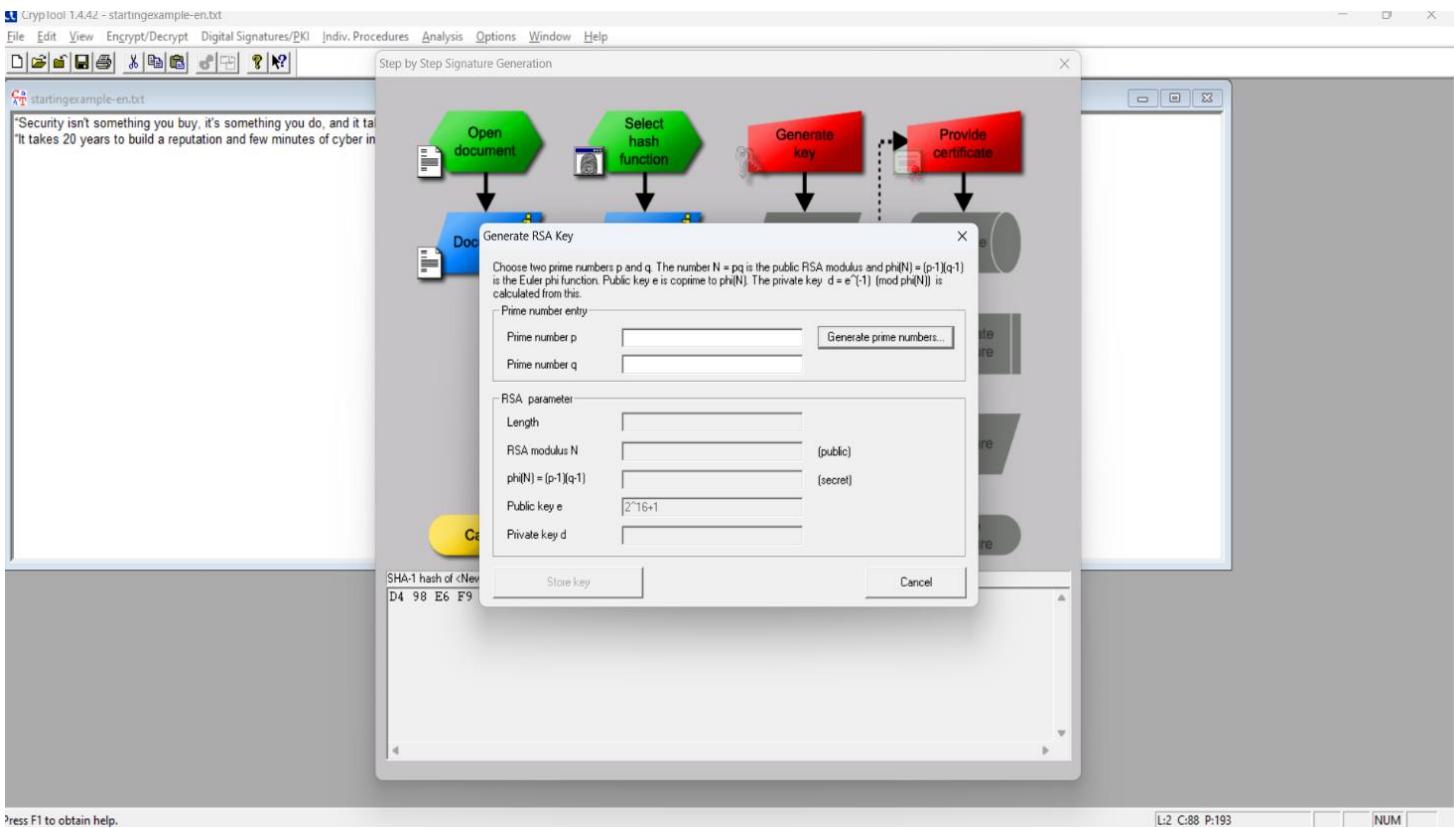
Encryption vs Decryption Histogram



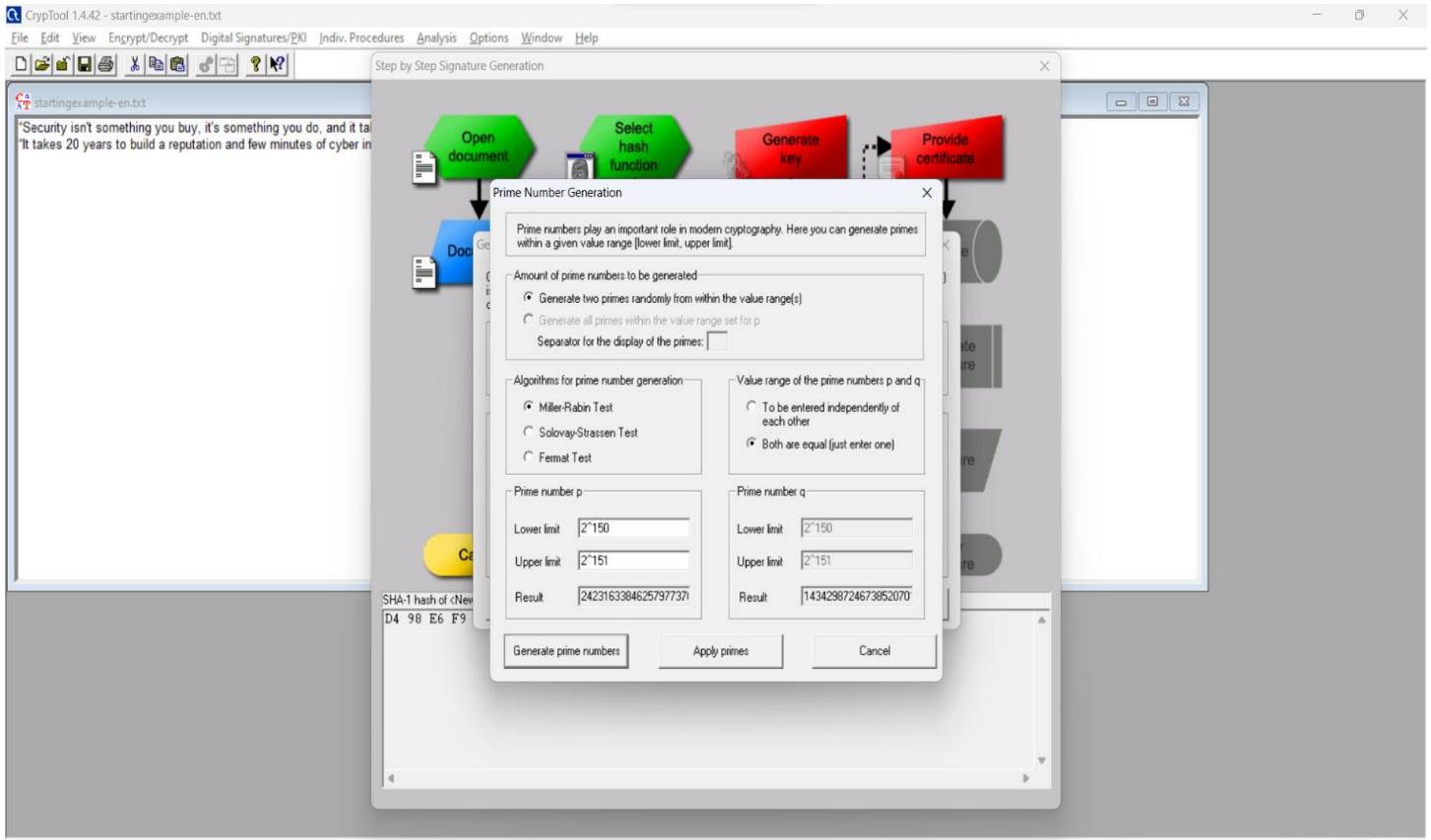
Digital Signature Process



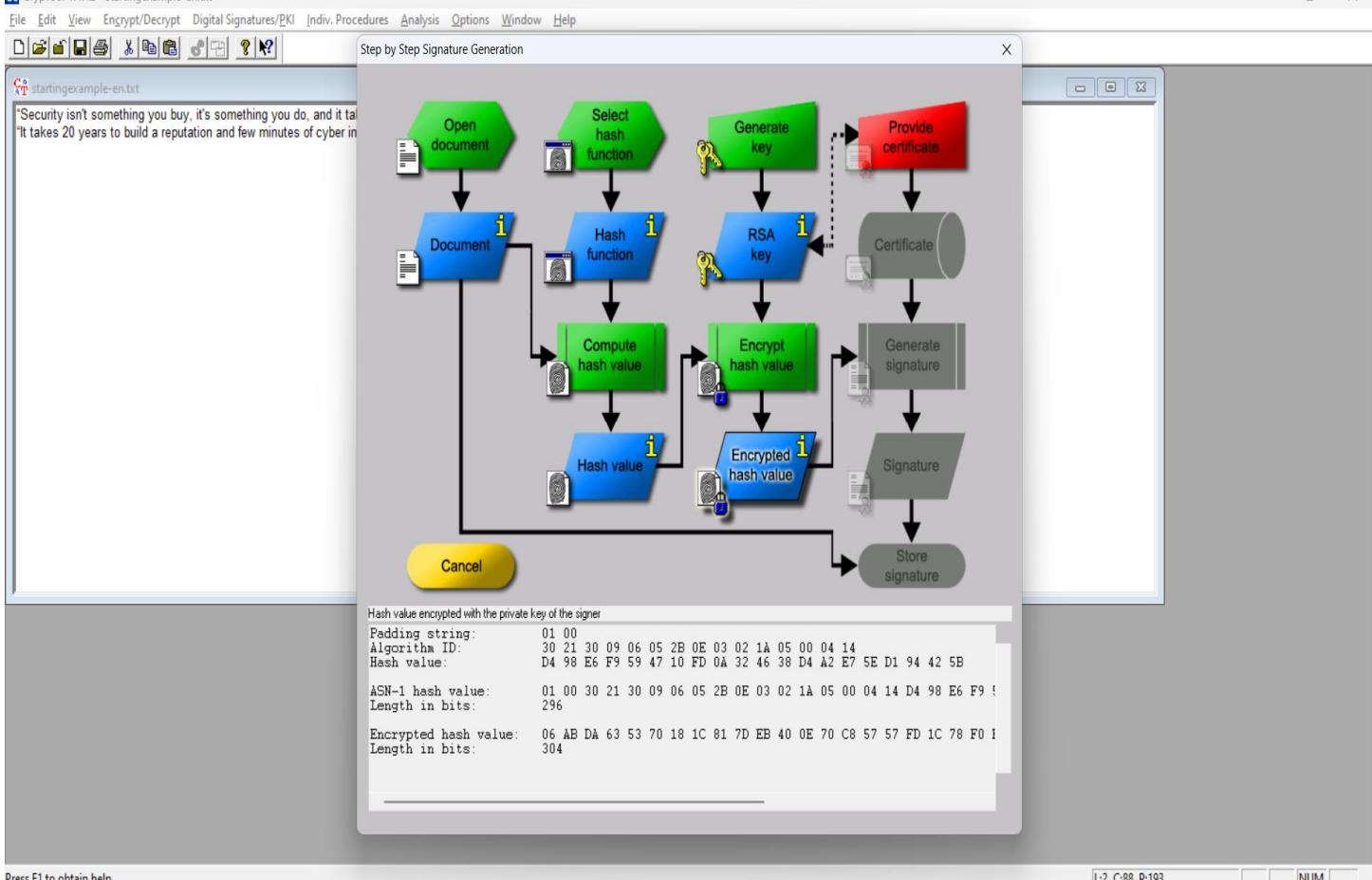
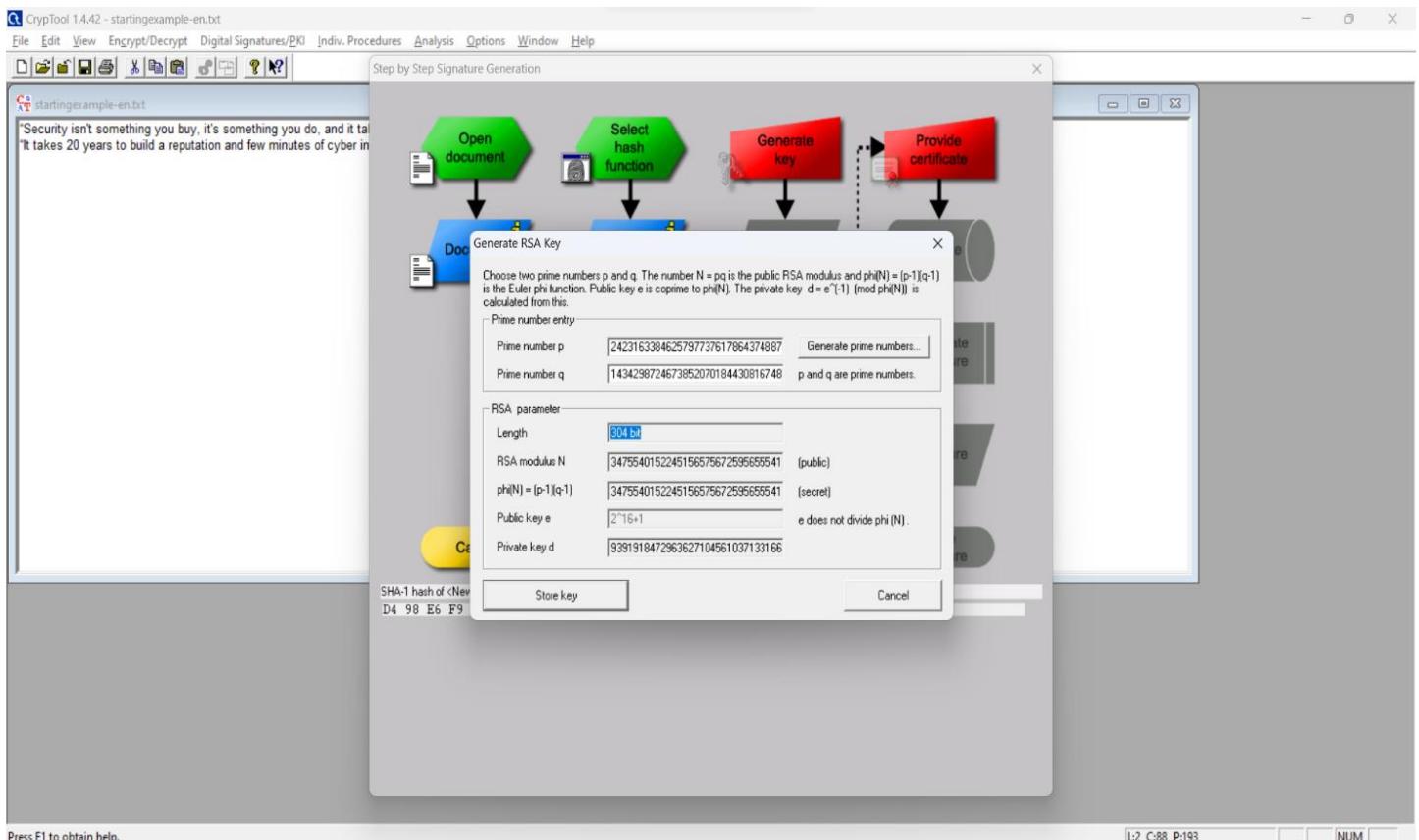


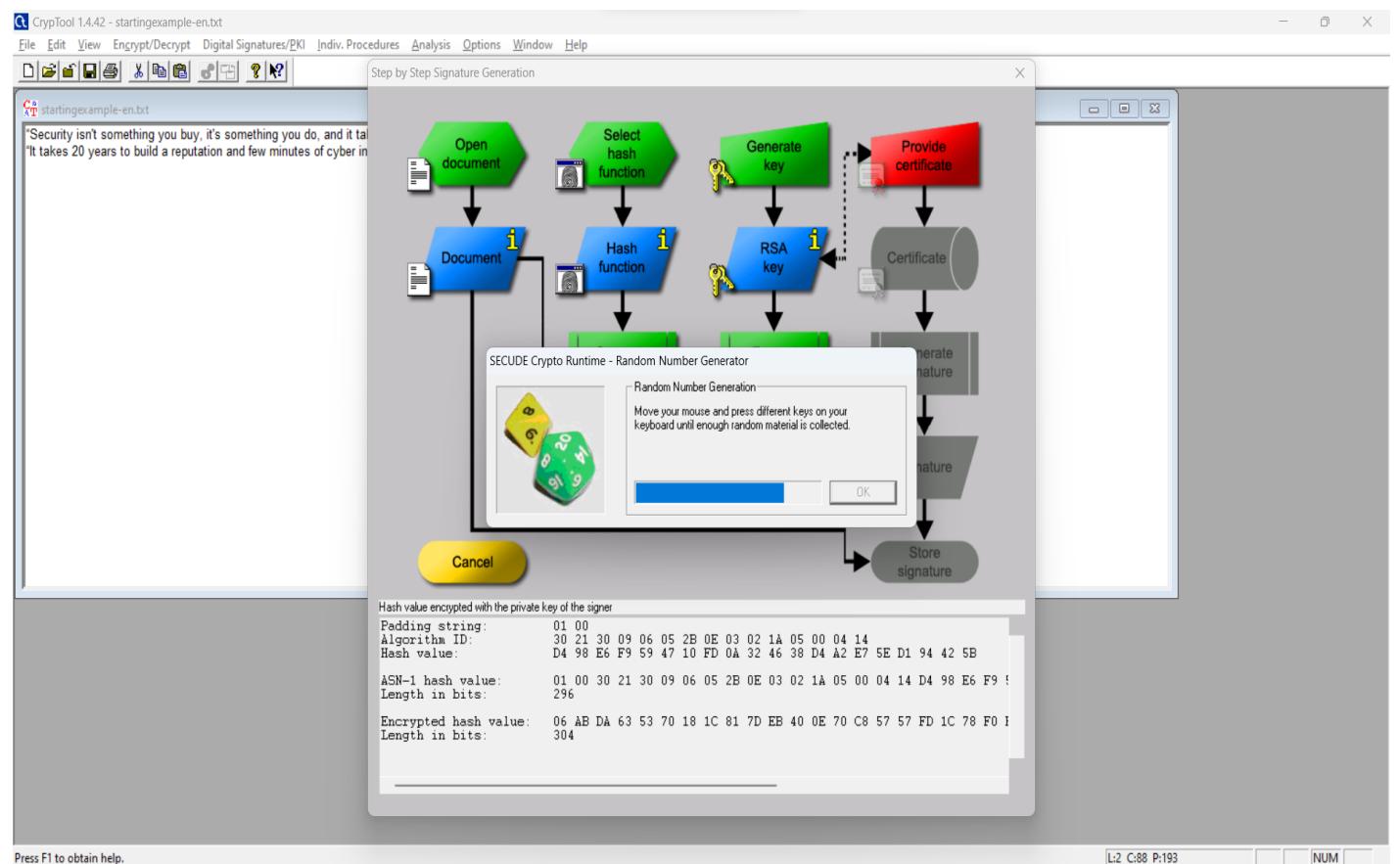
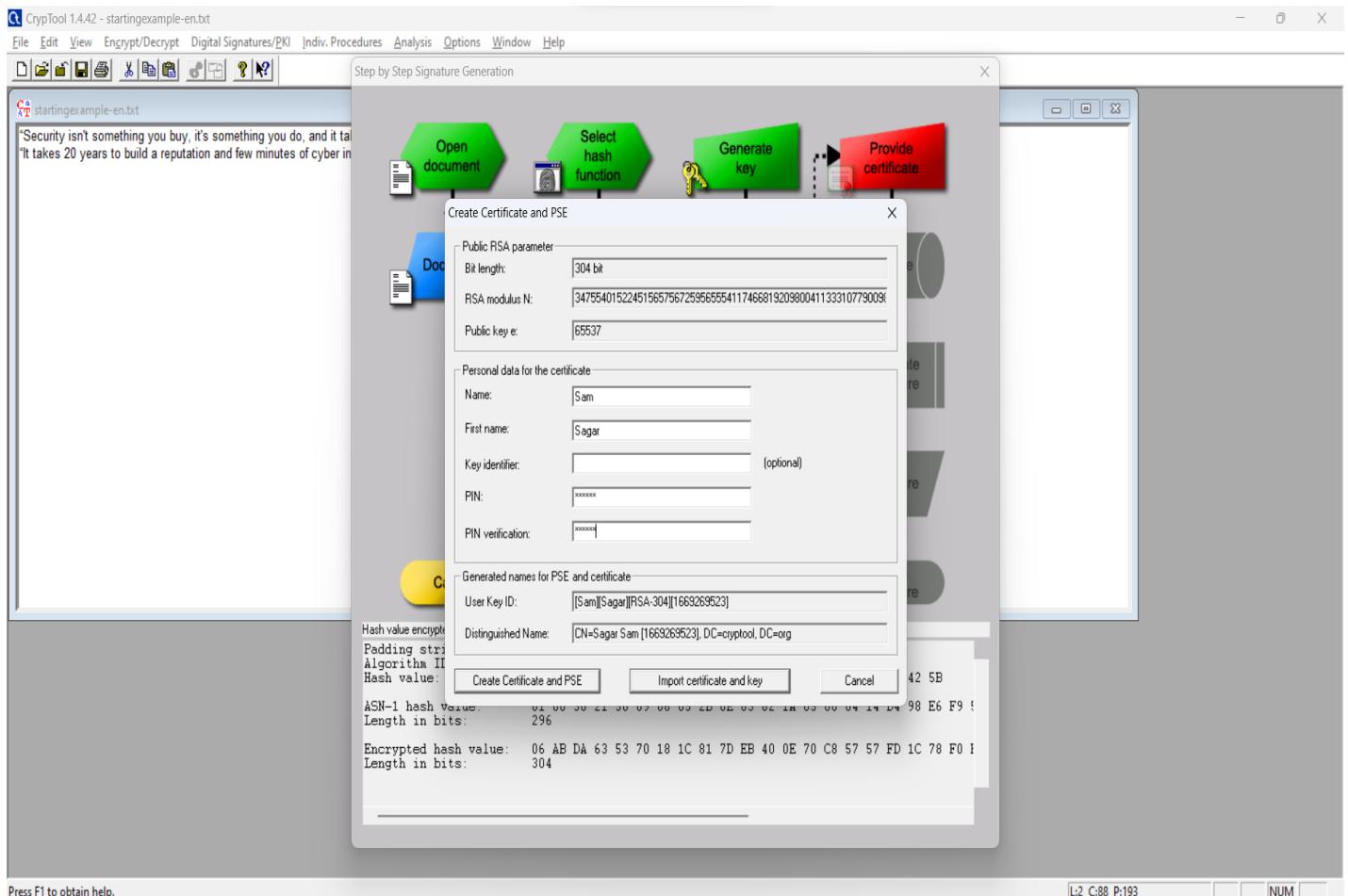


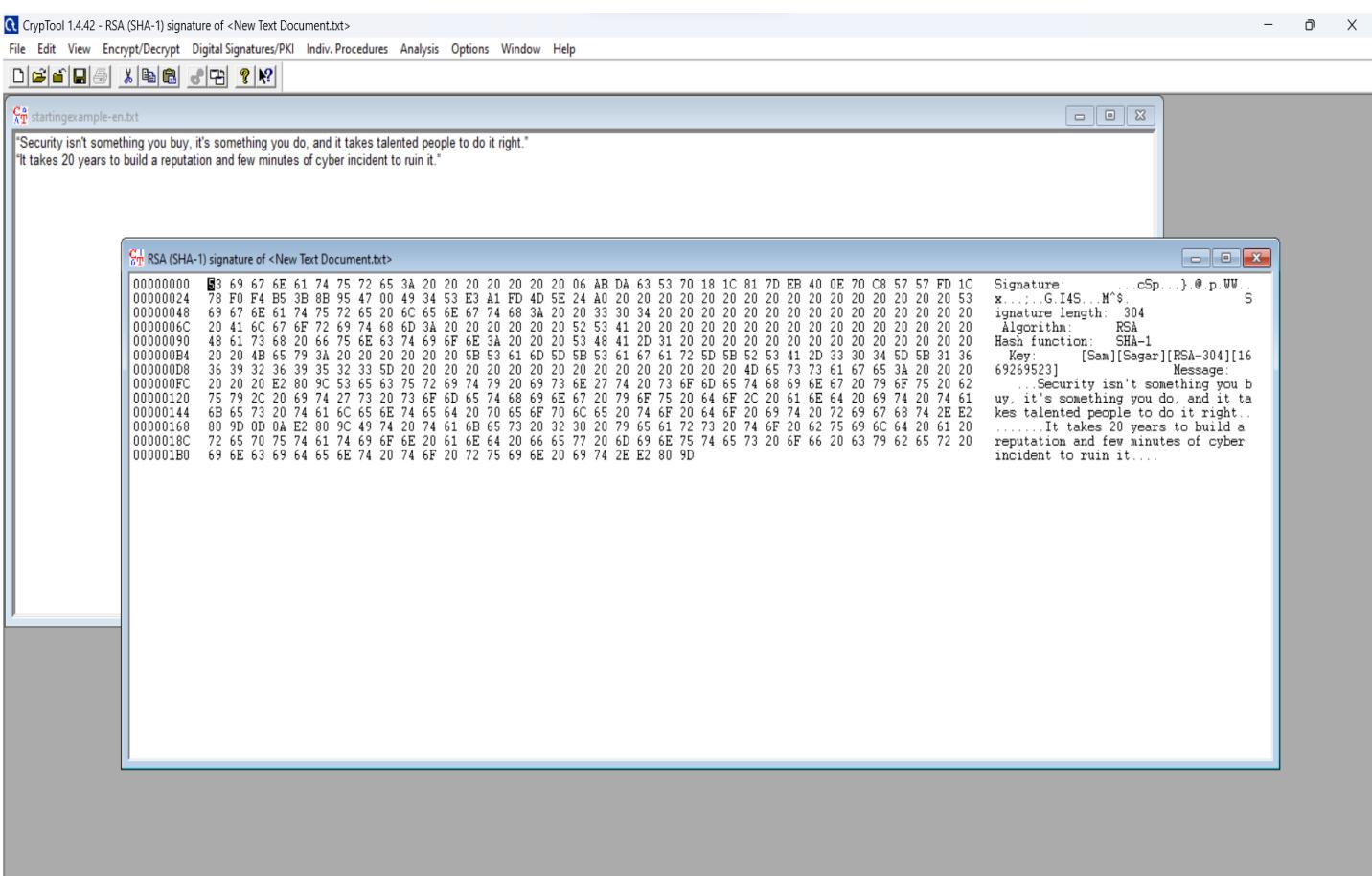
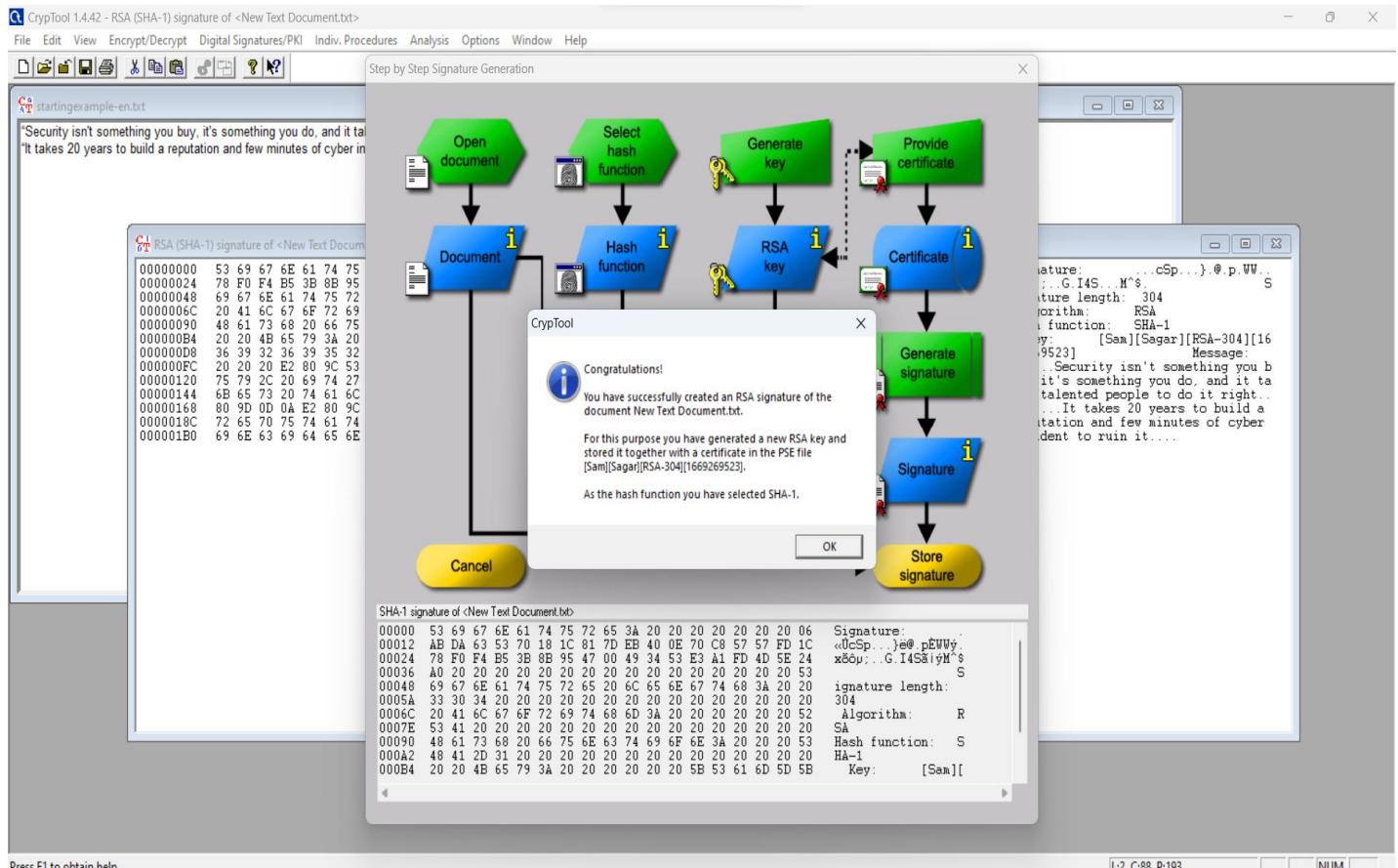
Press F1 to obtain help.



Press F1 to obtain help.







Assignment-4

Activity-1: Clone Google and Twitter homepage using set.

Open Kali linux

Go to Applications-> Social Engineering Tools-> Social Engineering Tool Kit (root)

Password for kali: kali

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HIA Attack Method

99) Return to Main Menu

set:webattack>3

File System

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1

```
File System  
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:1
```

***** Important Information *****

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

You can configure this option under:

```
/etc/setoolkit/set.config
```

```
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.
```

1. Java Required
2. Google
3. Twitter

```
set:webattack> Select a template:2
```

```
[*] Cloning the website: http://www.google.com  
[*] This could take a little bit...
```

```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.  
[*] The Social-Engineer Toolkit Credential Harvester Attack
```

```
[*] Credential Harvester is running on port 80
```

```
[*] Information will be displayed to you as it arrives below:
```

```
10.0.2.15 - - [24/Nov/2022 07:46:03] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [24/Nov/2022 07:46:04] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [24/Nov/2022 07:46:14] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [24/Nov/2022 07:46:15] "GET /favicon.ico HTTP/1.1" 404 -
```

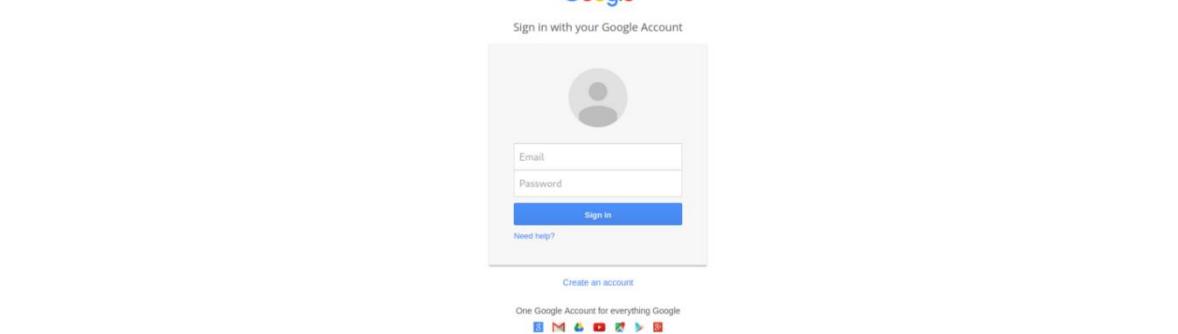
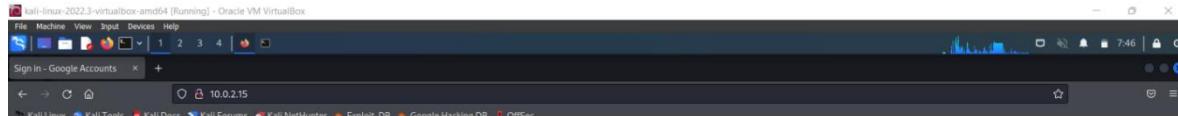


Image 1: cloned Google Sign In page

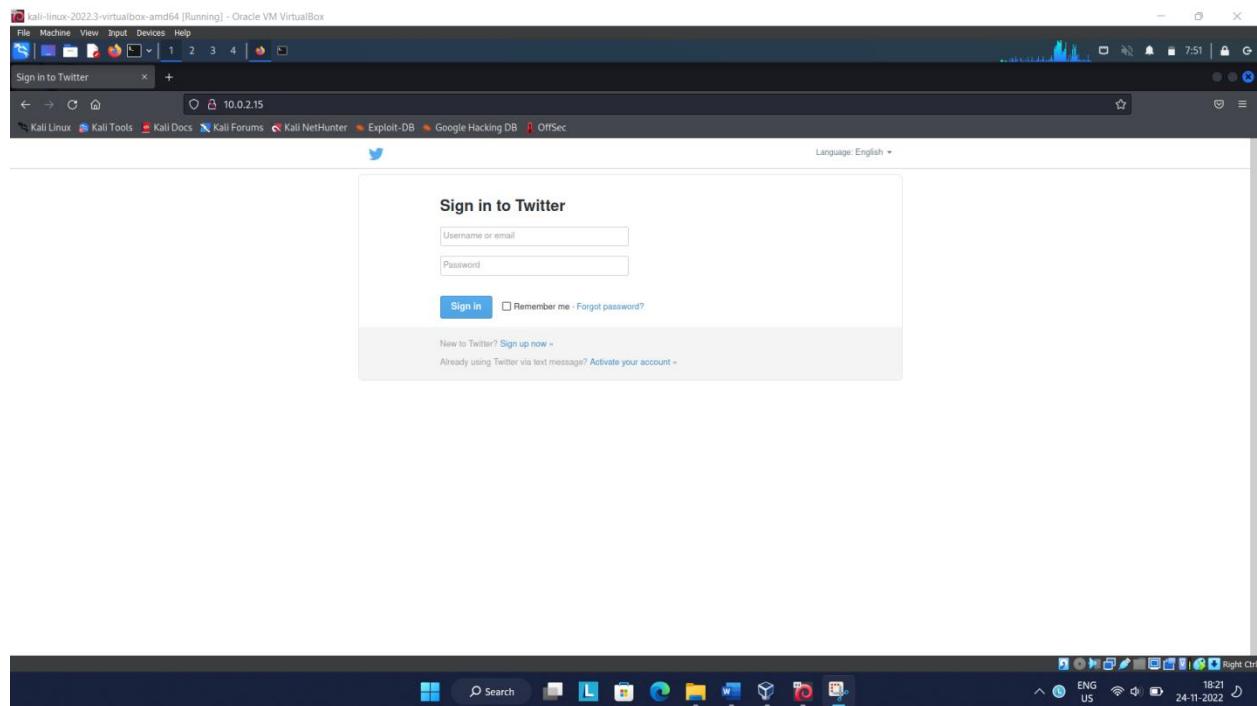
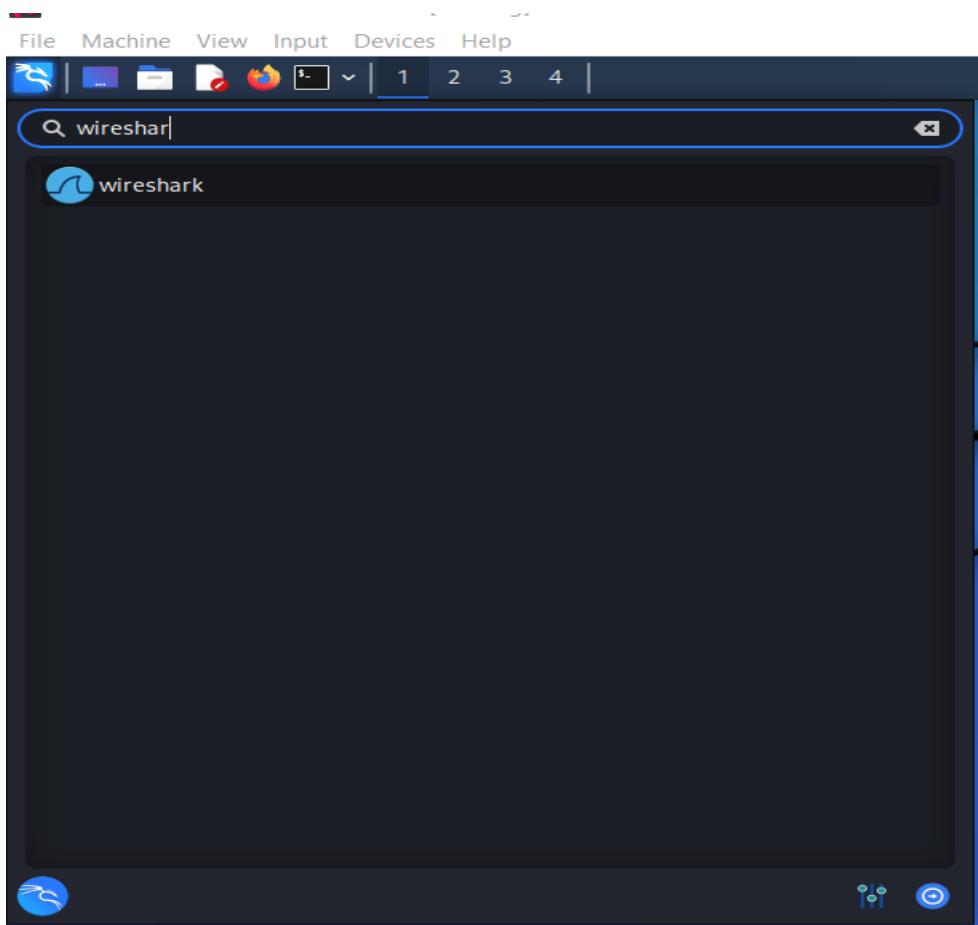


Image 2: Cloned Twitter Sign In page

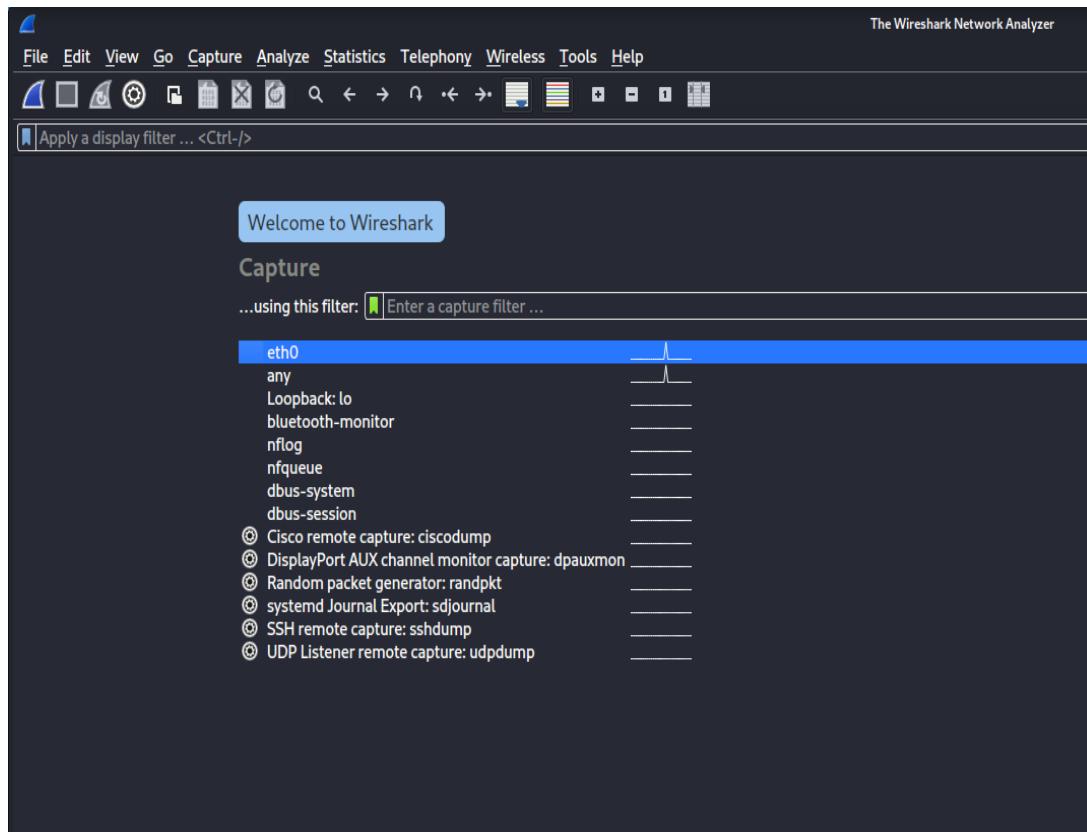
Termwork - 05

Steps in capturing packets in wireshark

1. Open wireshark and double click on any interface to start the packet capture process
2. Open browser and enter any websites fully qualified domain name in the browser address bar and hit enter.
3. After site is fully loaded , stop the capturing process in wireshark
4. Type the following in, apply the filter column and hit enter
`Tcp.flags.fin == 1 &&tcp.flags.ack == 1`
5. Select any one of this and hover on the conversion filter and select tcp. Once done
geeksforgeeks.com /wireshark tool

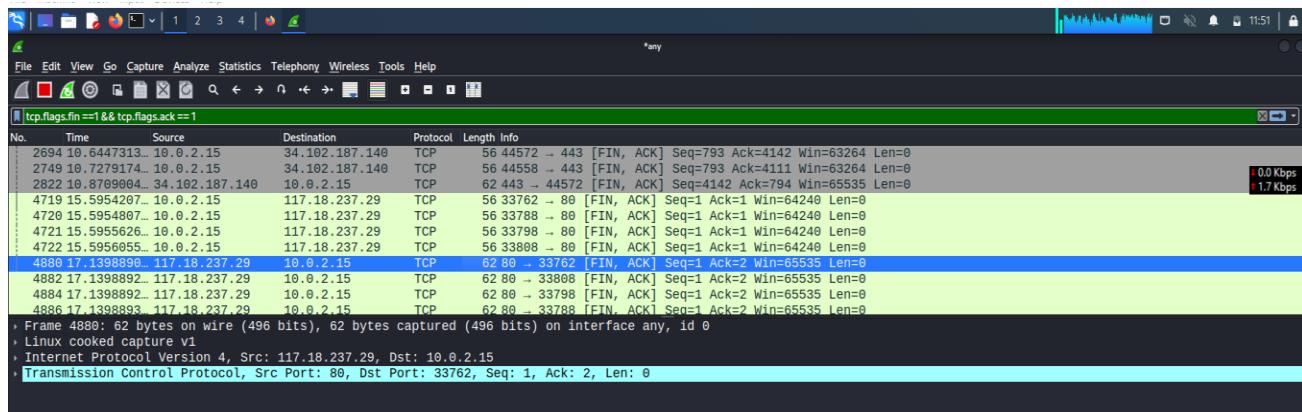


Search for wireshark in kali application



Click on Any

Open firefox and search any website



Wireshark starts capturing packets and we can apply filters (to know desired packets we required)